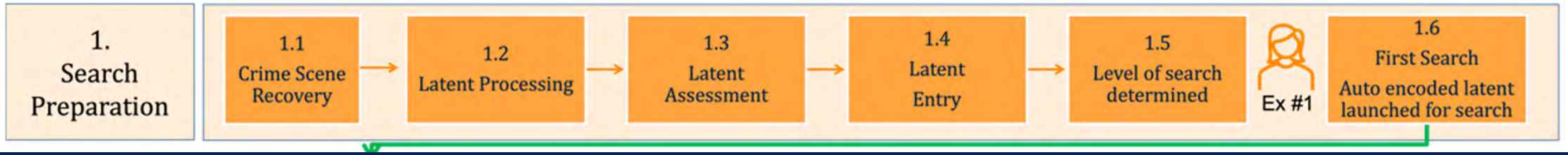
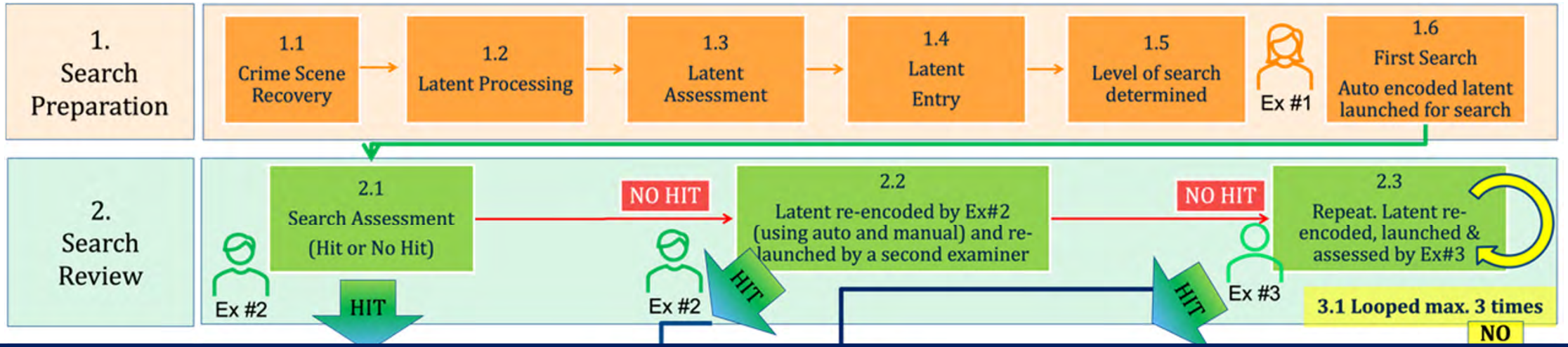
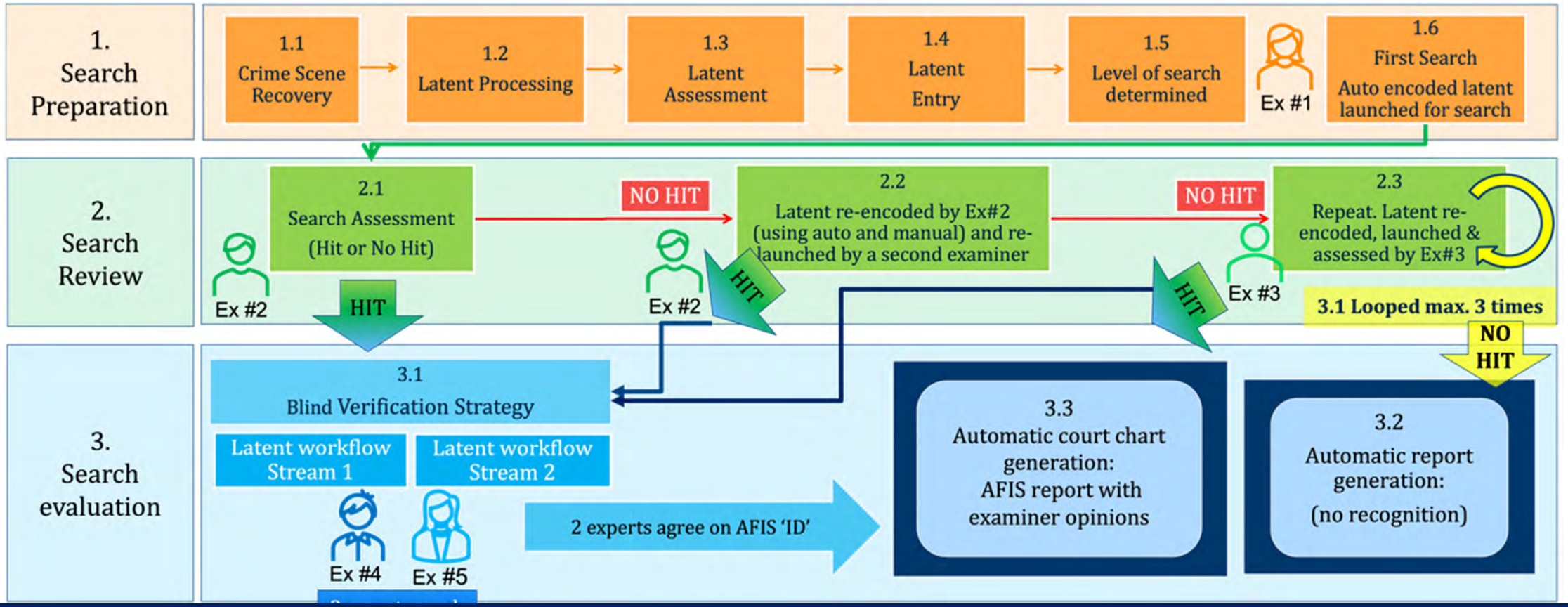
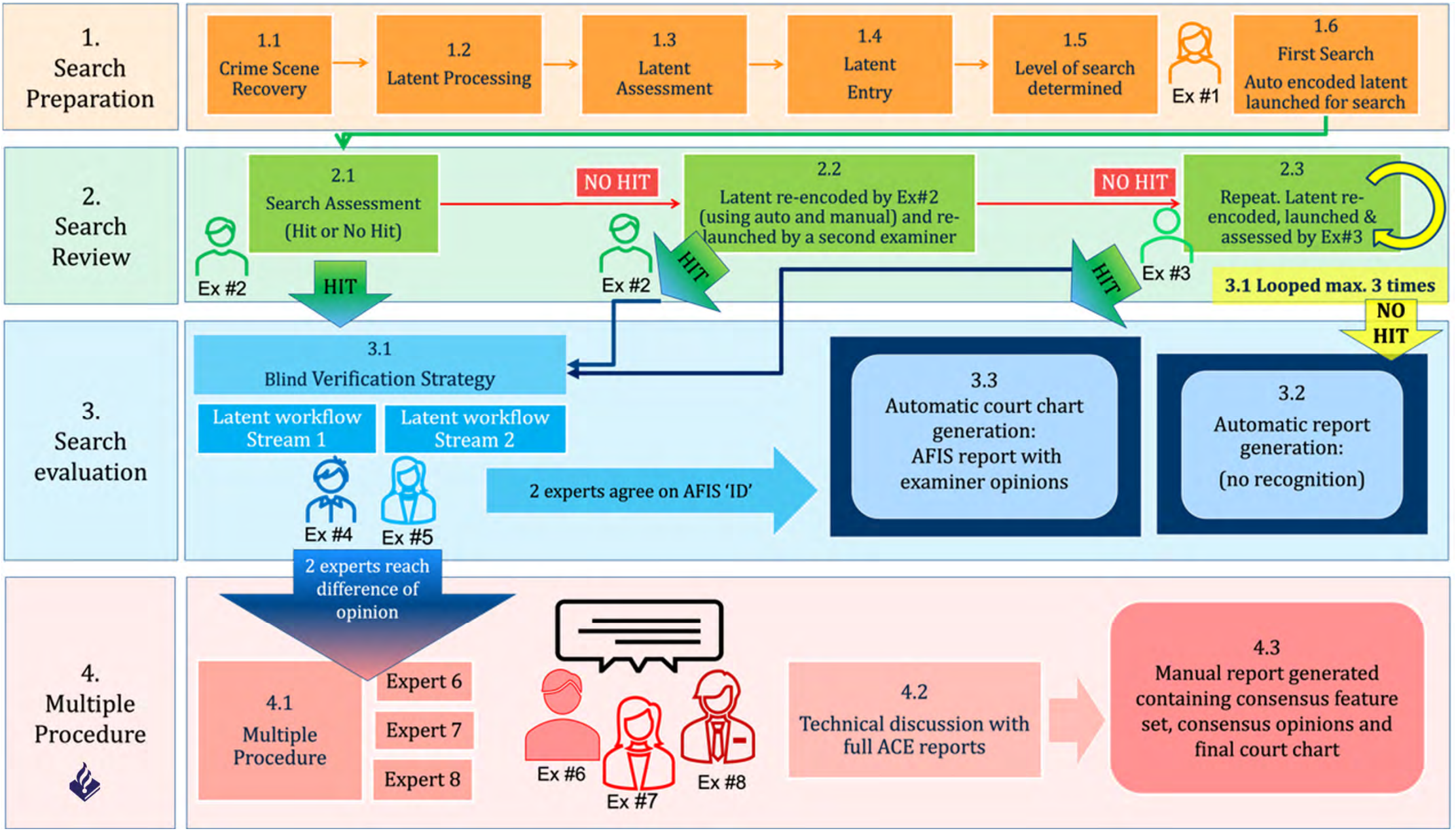
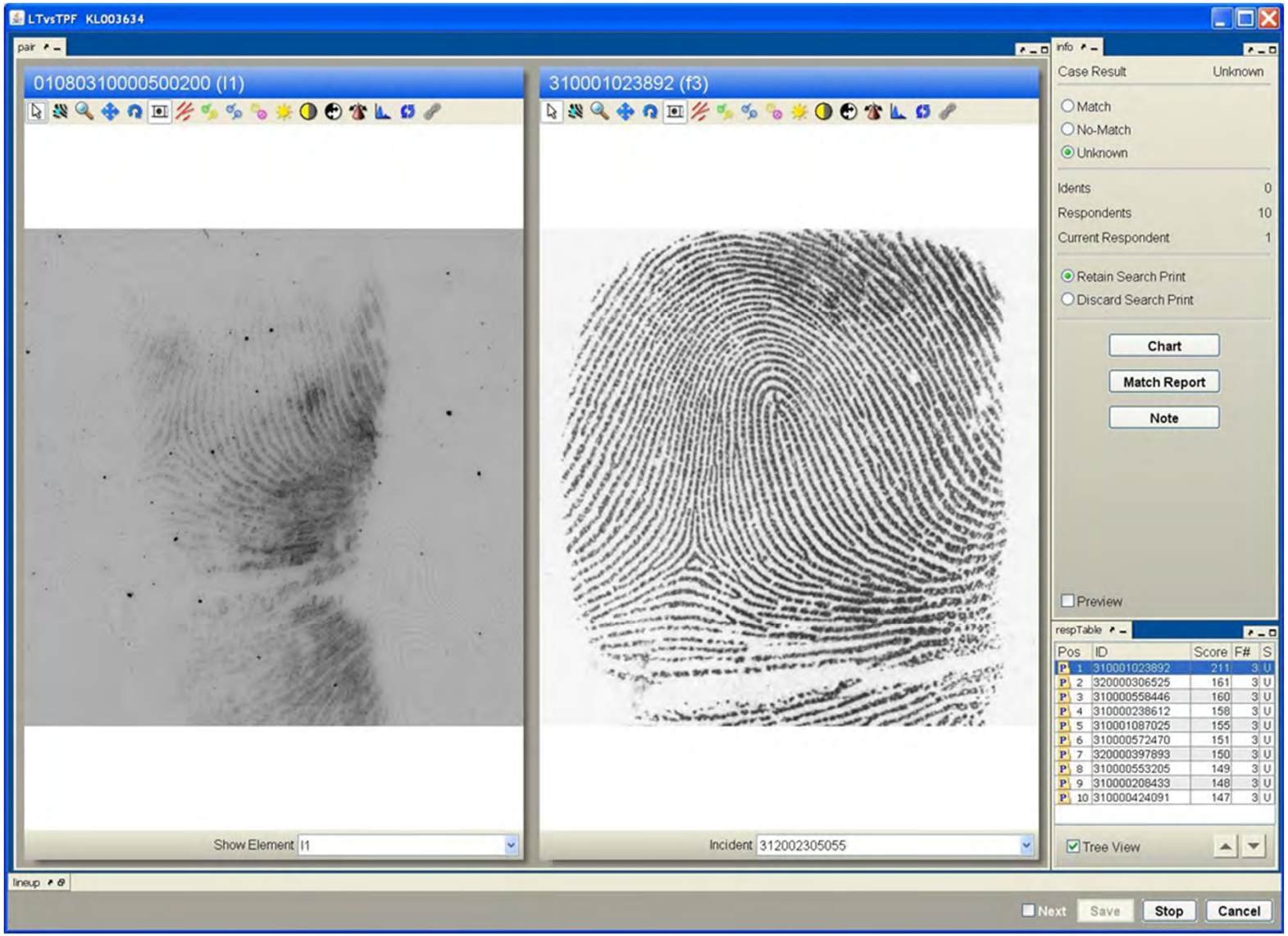

1.
Search
Preparation
1.1
Crime Scene
Recovery
1.2
Latent Processing
1.3
Latent
Assessment
1.4
Latent
Entry
1.5
Level of search
determined
Ex #1
1.6
First Search
Auto encoded latent
launched for search

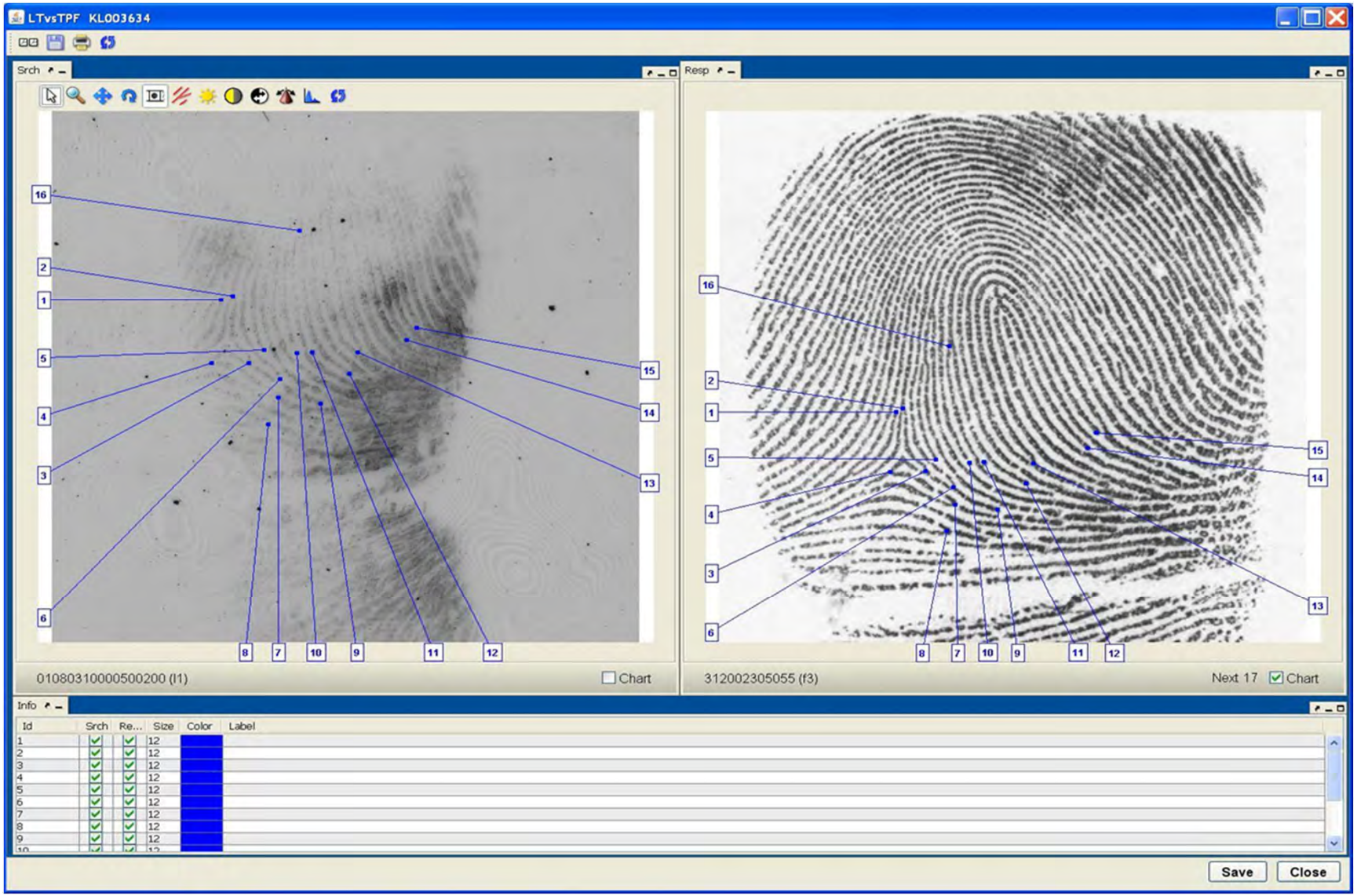

1.
Search
Preparation
1.1
Crime Scene
Recovery
1.2
Latent Processing
1.3
Latent
Assessment
1.4
Latent
Entry
1.5
Level of search
determined
Ex #1
1.6
First Search
Auto encoded latent
launched for search
2.
Search
Review
2.1
Search Assessment
(Hit or No Hit)
NO HIT
2.2
Latent re-encoded by Ex#2
(using auto and manual) and re-
launched by a second examiner
NO HIT
2.3
Repeat. Latent re-
encoded, launched &
assessed by Ex#3
Ex #2
HIT
Ex #2
HIT
HIT
Ex #3
3.1 Looped max. 3 times
NO

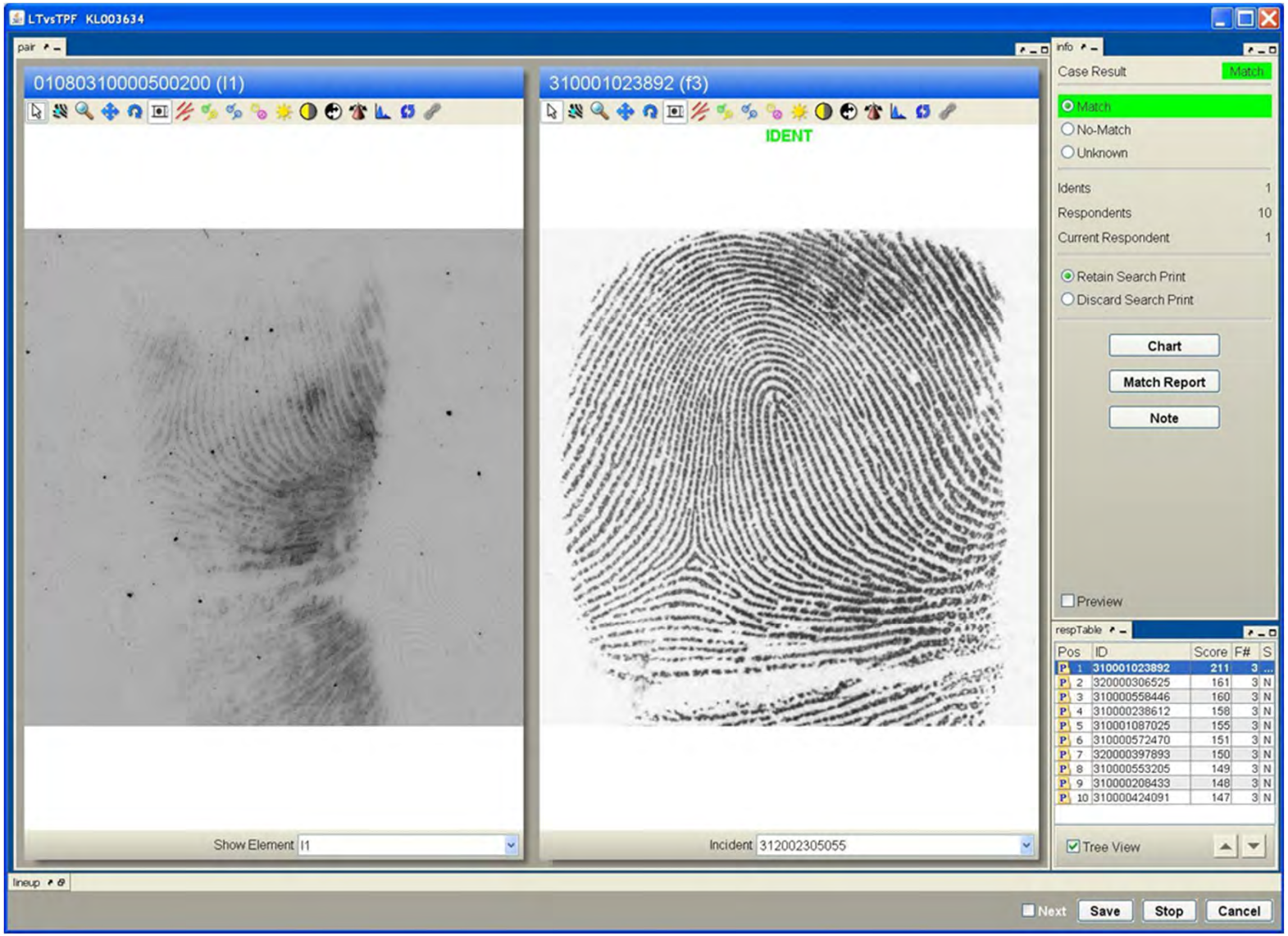

1. Search Preparation
1.1 Crime Scene Recovery
1.2 Latent Processing
1.3 Latent Assessment
1.4 Latent Entry
1.5 Level of search determined
Ex #1
1.6 First Search Auto encoded latent launched for search
2. Search Review
2.1 Search Assessment (Hit or No Hit)
Ex #2
HIT
NO HIT
2.2 Latent re-encoded by Ex#2 (using auto and manual) and re-launched by a second examiner
Ex #2
HIT
NO HIT
2.3 Repeat. Latent re-encoded, launched & assessed by Ex#3
Ex #3
HIT
3.1 Looped max. 3 times
NO HIT
3. Search evaluation
3.1 Blind Verification Strategy
Latent workflow Stream 1
Latent workflow Stream 2
Ex #4
Ex #5
2 experts agree on AFIS 'ID'
3.3 Automatic court chart generation: AFIS report with examiner opinions
3.2 Automatic report generation: (no recognition)

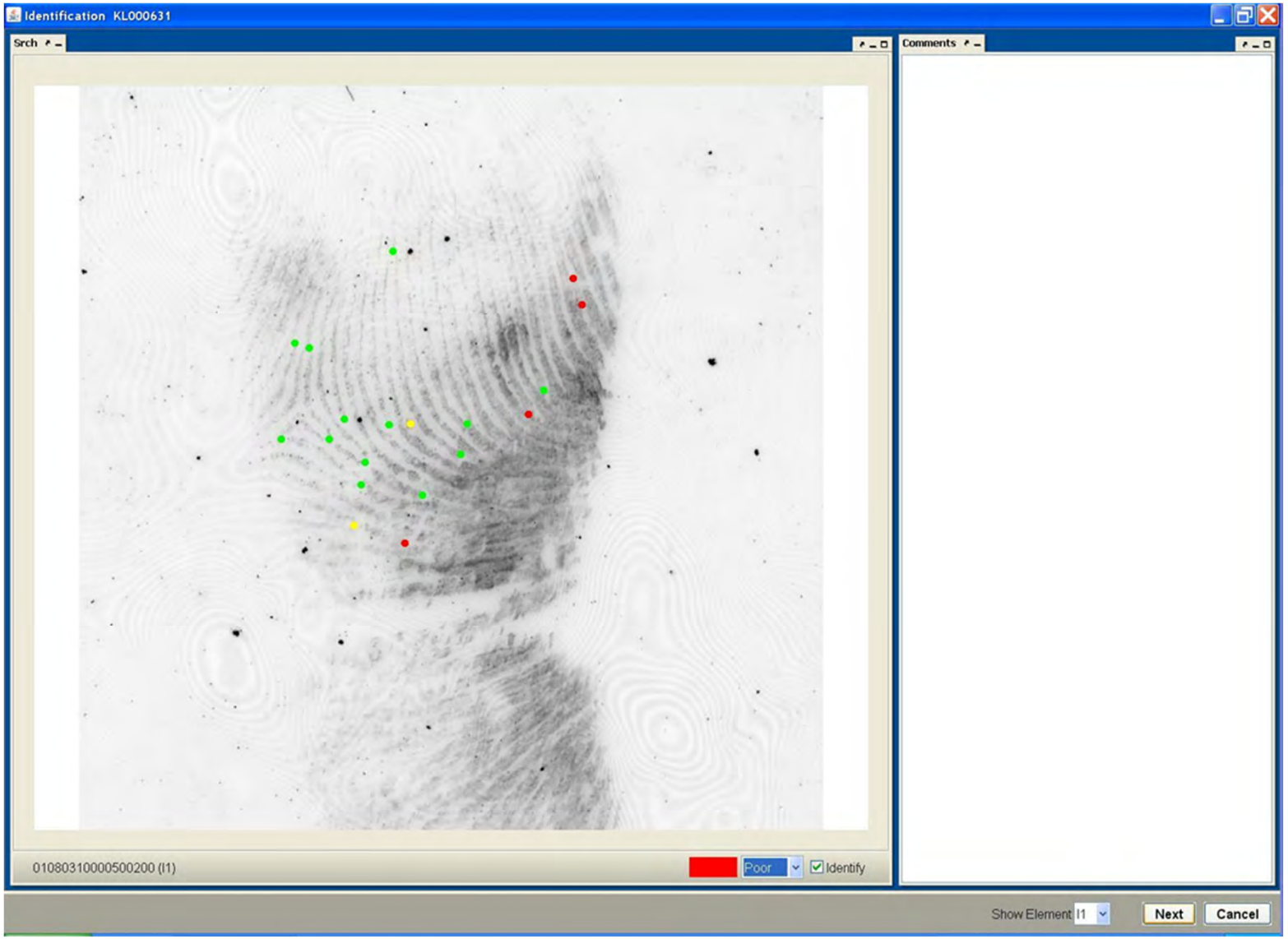

1. Search Preparation
1.1 Crime Scene Recovery
1.2 Latent Processing
1.3 Latent Assessment
1.4 Latent Entry
1.5 Level of search determined
Ex #1
1.6 First Search Auto encoded latent launched for search
2. Search Review
2.1 Search Assessment (Hit or No Hit)
Ex #2
HIT
NO HIT
2.2 Latent re-encoded by Ex#2 (using auto and manual) and re-launched by a second examiner
Ex #2
HIT
NO HIT
2.3 Repeat. Latent re-encoded, launched & assessed by Ex#3
Ex #3
HIT
3.1 Looped max. 3 times
NO HIT
3. Search evaluation
3.1 Blind Verification Strategy
Latent workflow Stream 1
Latent workflow Stream 2
Ex #4
Ex #5
2 experts agree on AFIS 'ID'
3.3 Automatic court chart generation: AFIS report with examiner opinions
3.2 Automatic report generation: (no recognition)
2 experts reach difference of opinion
4. Multiple Procedure
4.1 Multiple Procedure
Expert 6
Expert 7
Expert 8
Ex #6
Ex #7
Ex #8
4.2 Technical discussion with full ACE reports
4.3 Manual report generated containing consensus feature set, consensus opinions and final court chart

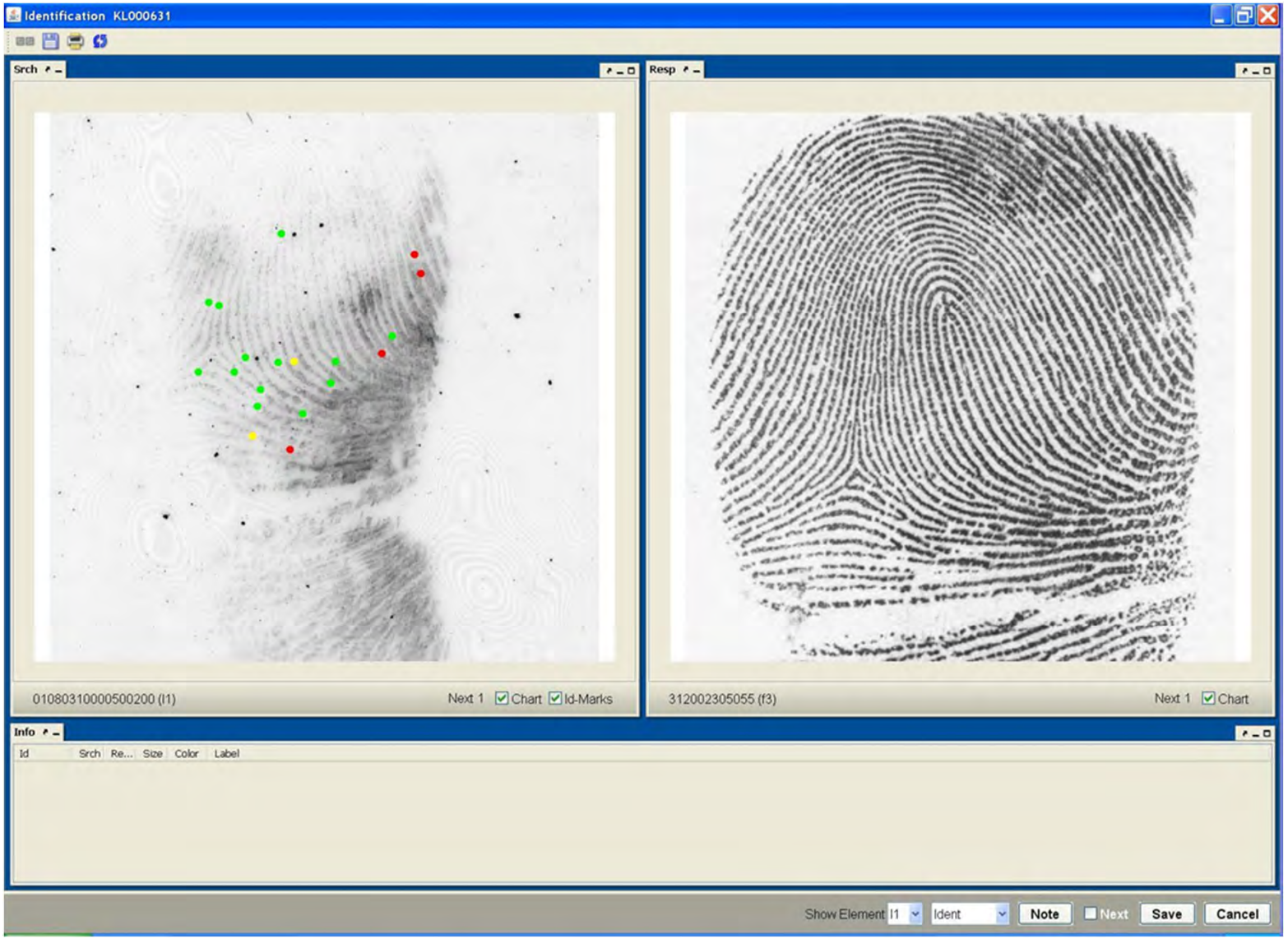
Hoe ziet dat er dan uit?

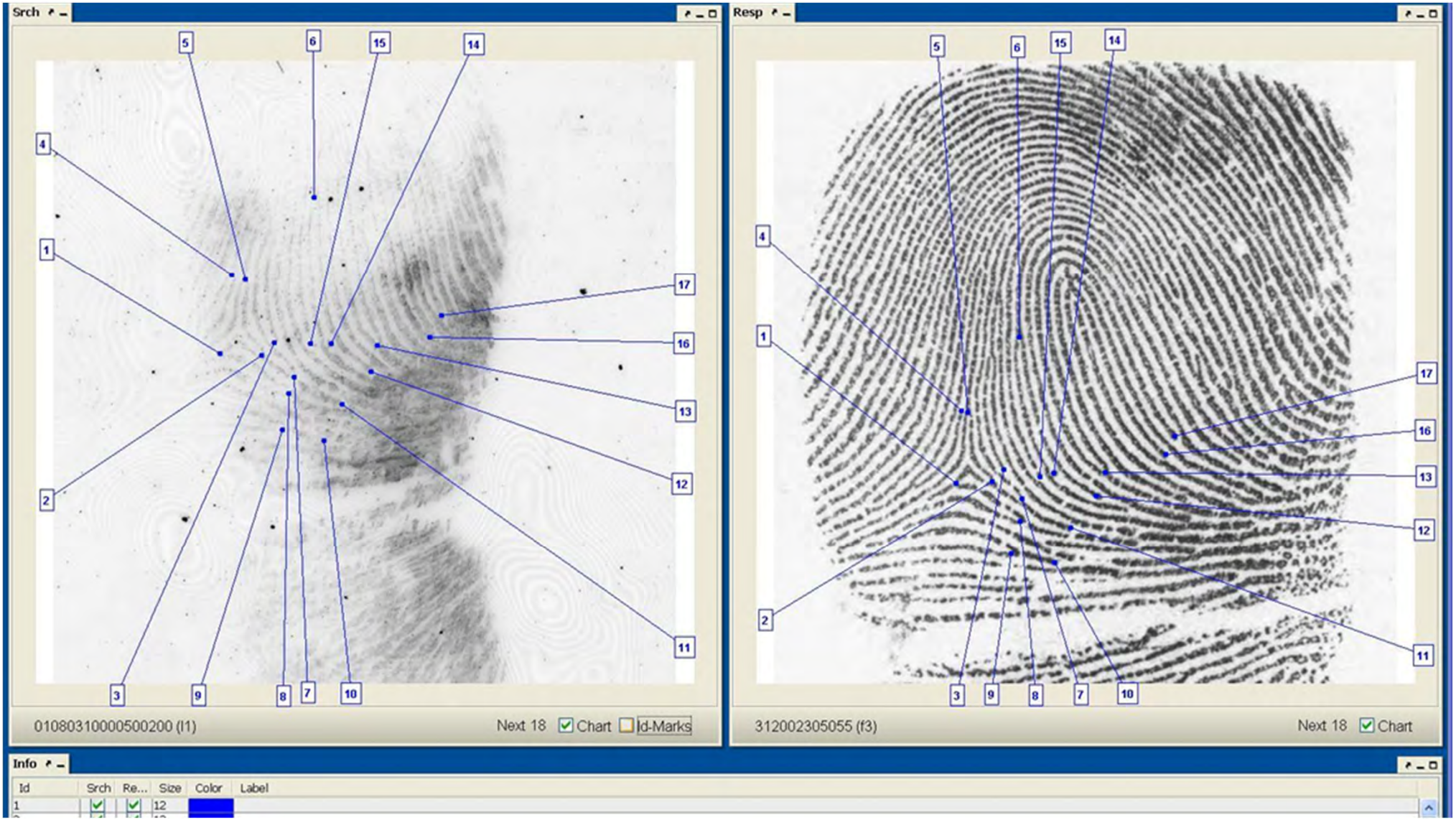

LTvsTPF KL003634
pair
01080310000500200 (I1)
310001023892 (f3)
Show Element I1
Incident 312002305055
info
Case Result Unknown
Match
No-Match
Unknown
Idents 0
Respondents 10
Current Respondent 1
Retain Search Print
Discard Search Print
Chart
Match Report
Note
Preview
respTable
Pos ID Score F# S
1 310001023892 211 3 U
2 320000306525 161 3 U
3 310000558446 160 3 U
4 310000238612 158 3 U
5 310001087025 155 3 U
6 310000572470 151 3 U
7 320000397893 150 3 U
8 310000553205 149 3 U
9 310000208433 148 3 U
10 310000424091 147 3 U
Tree View
lineup
Next
Save
Stop
Cancel


LTvsTPF KL003634
Srch
Resp
01080310000500200 (I1)
Chart
312002305055 (f3)
Next 17
Chart
Info
Id
Srch
Re...
Size
Color
Label
Save
Close


LTvsTPF KL003634
pair
01080310000500200 (I1)
310001023892 (f3)
IDENT
Show Element I1
Incident 312002305055
info
Case Result
Match
Match
No-Match
Unknown
Idents 1
Respondents 10
Current Respondent 1
Retain Search Print
Discard Search Print
Chart
Match Report
Note
Preview
respTable
Pos ID Score F# S
1 310001023892 211 3
2 320000306525 161 3 N
3 310000558446 160 3 N
4 310000238612 158 3 N
5 310001087025 155 3 N
6 310000572470 151 3 N
7 320000397893 150 3 N
8 310000553205 149 3 N
9 310000208433 148 3 N
10 310000424091 147 3 N
Tree View
lineup
Next
Save
Stop
Cancel


Identification KL000631
Srch
Comments
01080310000500200 (I1)
Poor
Identify
Show Element I1
Next
Cancel


Identification KL000631
Srch
Resp
01080310000500200 (I1)
Next 1
Chart
Id-Marks
312002305055 (f3)
Next 1
Chart
Info
Id
Srch
Re...
Size
Color
Label
Show Element
I1
Ident
Note
Next
Save
Cancel

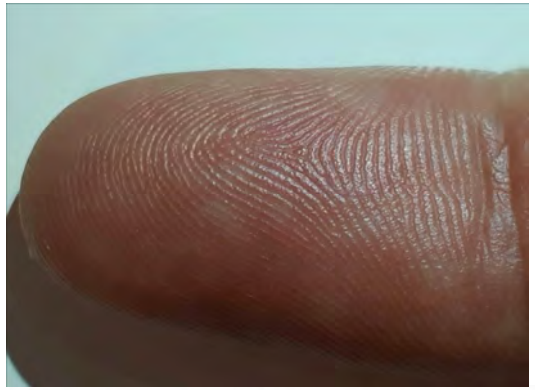

Srch
Resp
01080310000500200 (I1)
Next 18
Chart
Id-Marks
312002305055 (f3)
Next 18
Chart
Info
Id
Srch
Re...
Size
Color
Label
1
12

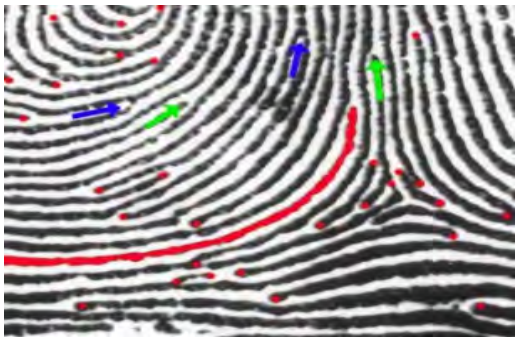
Hoeveel informatie is nodig om tot een conclusie te komen?

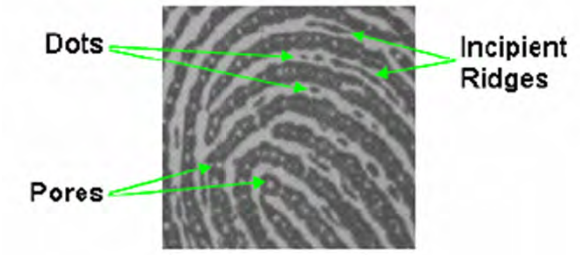
Eerste niveau van informatie– classificatie (lus, boog, kring)

Tweede niveau van informatie– Minutiae

Derde niveau van informatie – Lijnranden, poriën,







Nederlandse politie standaard voor vingerafdrukken

Holistische numerieke benadering

10 – 12 overeenkomstige minutiae

Aanvullende informatie in het spoor (derde niveau, opmerkelijke gebeurtenissen etc)

Geen absolute conclusies

Conclusies (8)

1. Spoor is niet geschikt voor onderzoek
2. Spoor is van getuige
3. Spoor is niet herkend
4. Spoor is niet van de potentiële donor (na ACE-ACE)
5. Individualisatie(standaard)
6. Geen individualisatie , het spoor is mogelijke afkomstig van potentiële donor (na ACE ACE))
7. Geen overtuigende conclusie
8. Referentie afdruk (tenprint) is van onvoldoende kwaliteit

POLITIE

RAPPORT DACTYLOSCOPISCH SPORENONDERZOEK

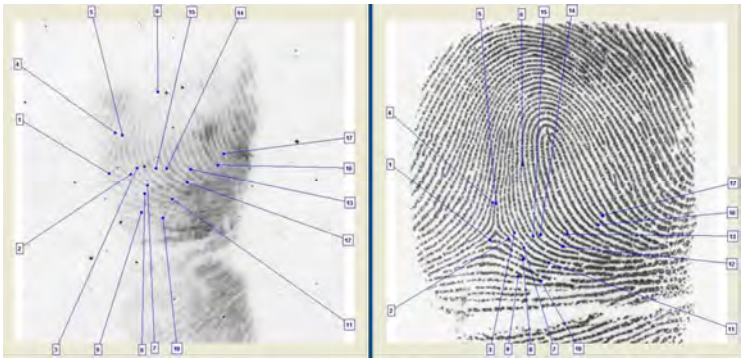
Dactyloscopisch onderzoek:

Met de afbeelding van dactyloscopisch spoor bekend in Havank onder nummer
is een vergelijkend onderzoek uitgevoerd in het actieve vinger-/handpalmafdrukkenbestand in HAVANK.

Bij de aanvraag werden de volgende gegevens vastgelegd:

Datum Invoer:
Kenmerk aanvrager:
Kenmerk Havank:
Zaakskenmerk:
Kenmerk sporendrager:

Accreditatie:



CATCH – Gelaatsvergelijking

Gelijk process voor galaatsvergelijking met een paar uitzonderingen

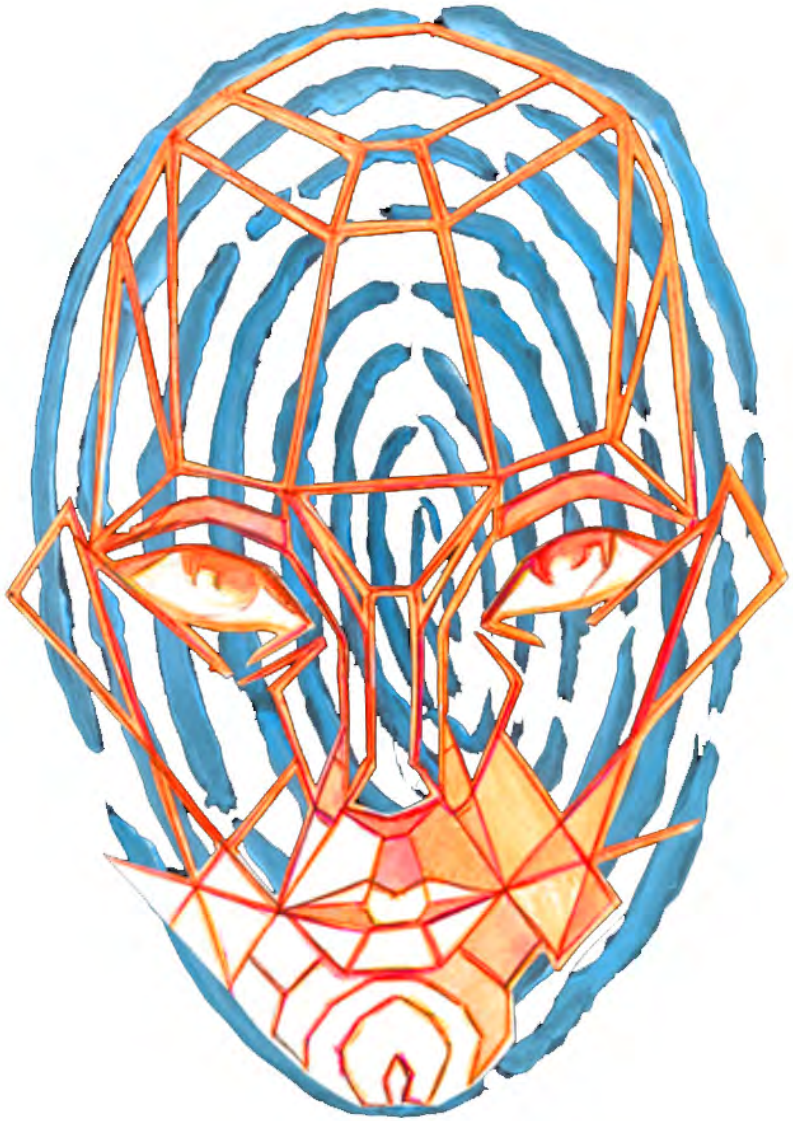
Hoe het begonnen is...

Opkomende problemen en uitdagingen

Geen grens aan criminaliteit– mobiliteit van criminelen

Digitale samenleving– Smartphones, laptops, CCTV, Social Media en big data

Identiteit blijft leidend– opsporingsindicaties



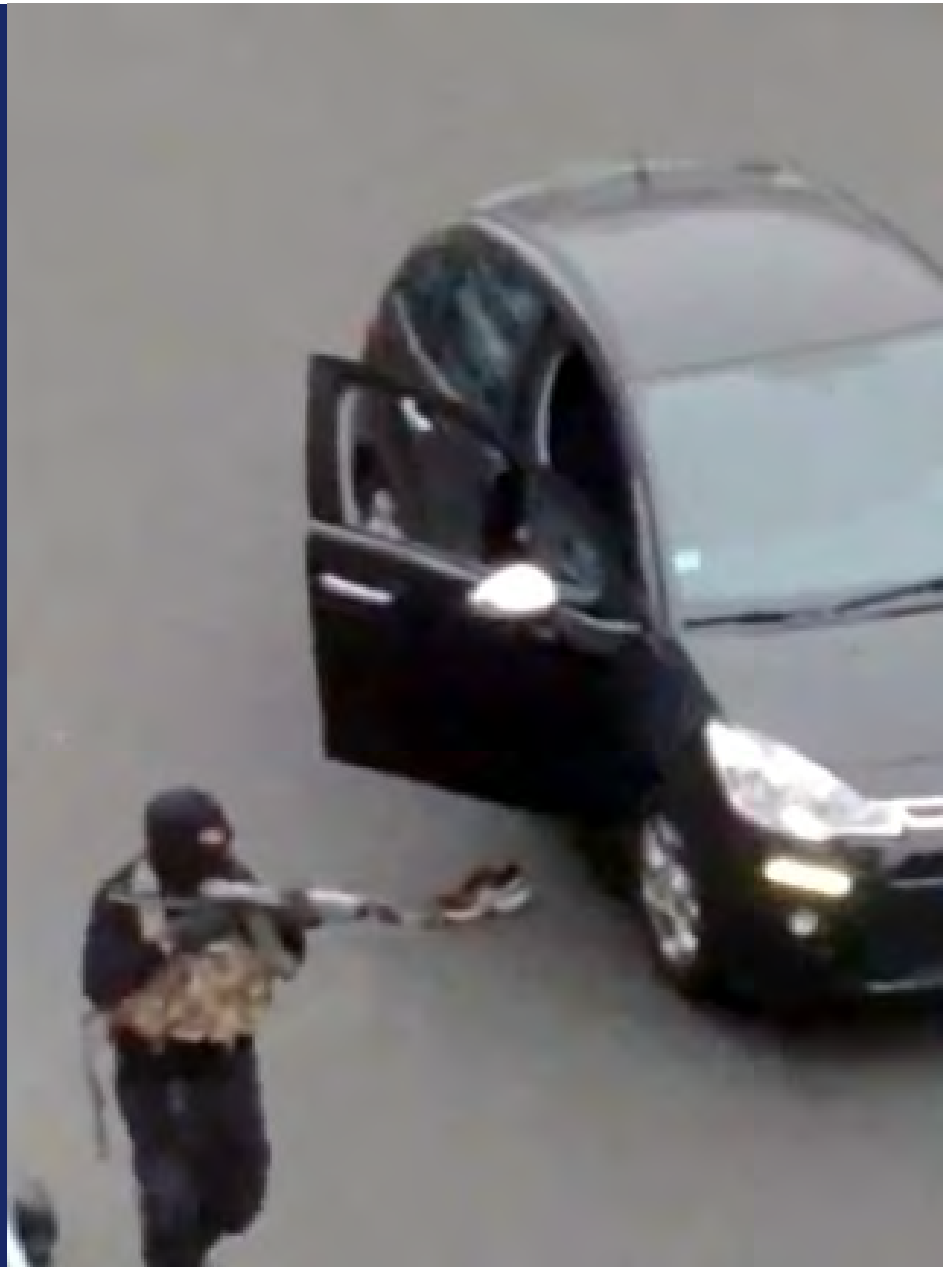
Ontstaan en gebruik

2014 – Pilot

2015 – Opdracht versneld implementeren

2016 / 2022 – Operationeel gebruik

2022 / 2023 – Implementatie CATCH 2.0



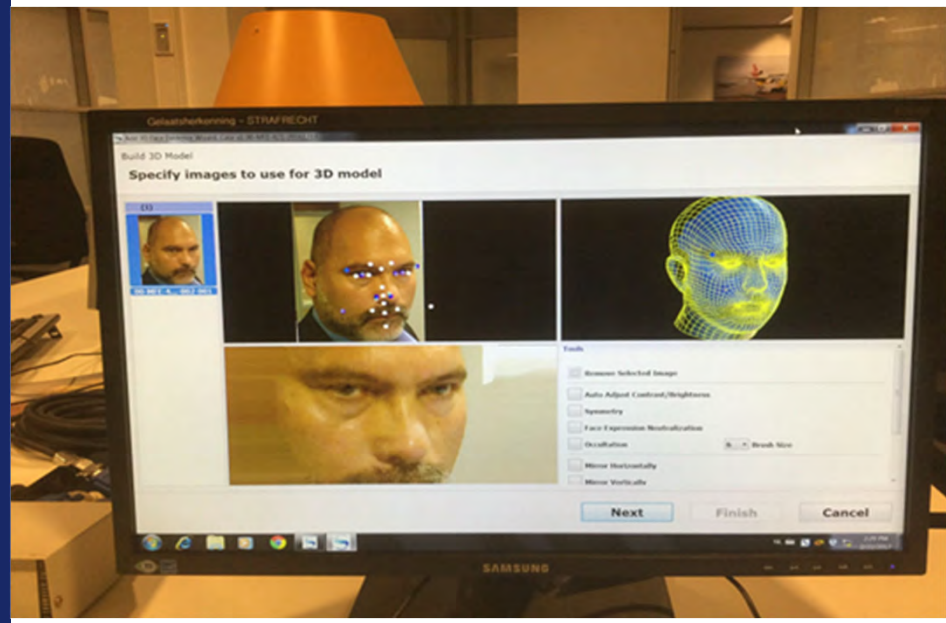
CATCH – Strafrecht

Vingerafdrukken en foto’s worden afgenomen ter vaststelling en vastlegging identiteit

Maar

Art. 55c, lid 4 WvSv;

De vingerafdrukken en foto’s mogen ook worden gebruikt voor het voorkomen, opsporen, vervolgen en berechten van strafbare feiten



CATCH – Vreemdelingen

Vingerafrukken en foto’s mogen ook wordne gebruikt **voor het opsporen en vervolgen van (VH)misdrijven**

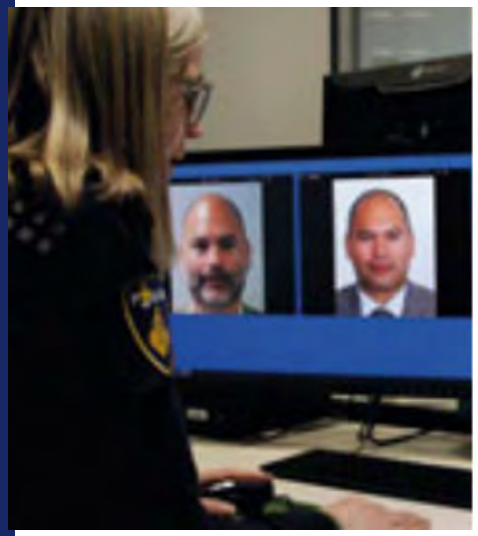
Art 107, lid 5, sub c, Vreemdelingewet 2000 (vreemdelingenwet 2000)

Vordering OvJ met een machtiging van de RC

De gezichtsvergelijkingsexpert

Rol

- Kwaliteitscontrole aangeboden materiaal
- Eventueel opwerken van het materiaal
- Zoeken en vergelijken (Double blind ACE-V)
- Concluderen



Holistisch vs Morfologische vergelijking

Holistisch

Gehele gezicht

Gehele vergelijking

Proporties

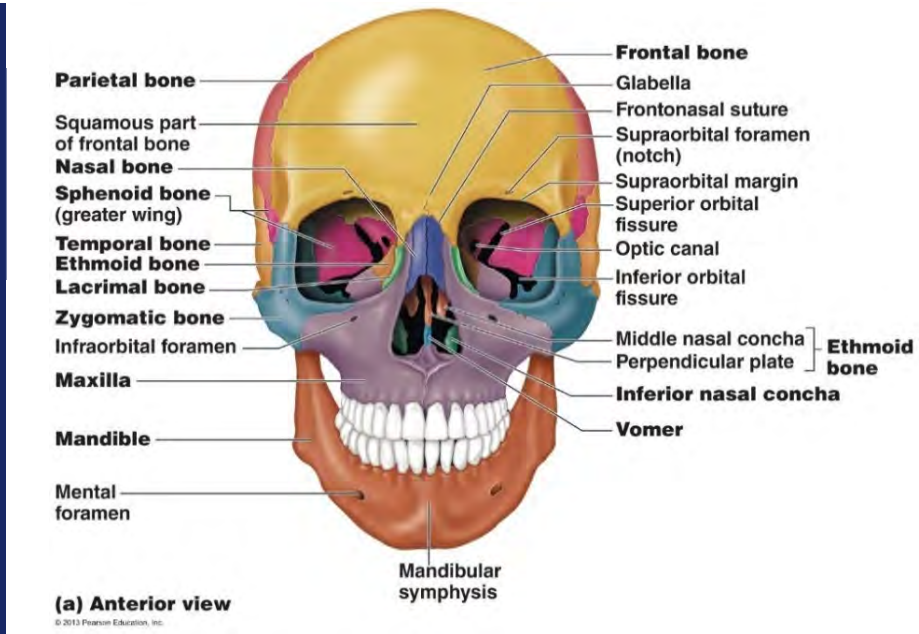
Snel

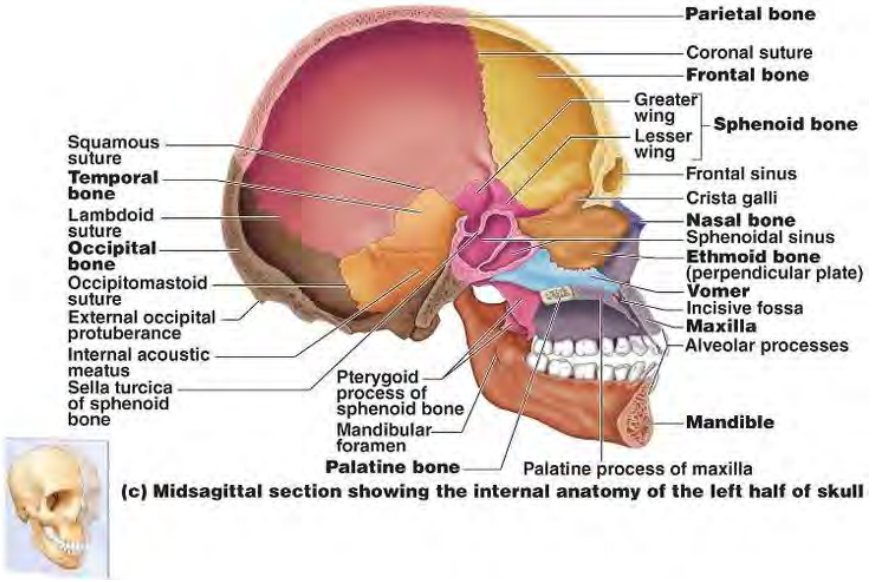
Morfologisch

Specifieke onderdelen van het gezicht

Hoger niveau van detail

Gedegen vergelijking van de onderdelen





Conclusies

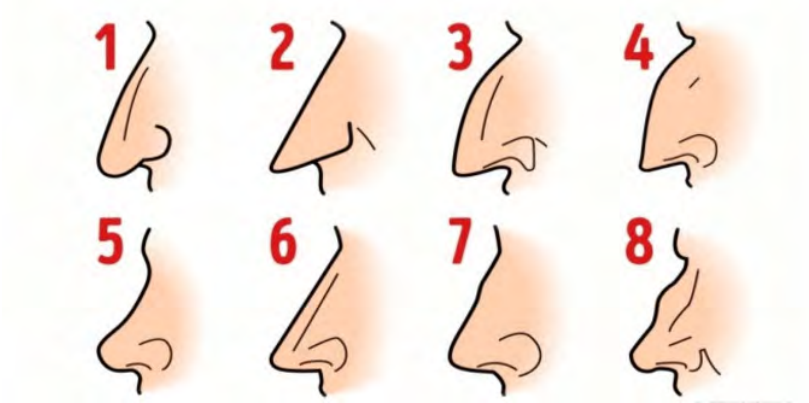
Rapporten met een indicatie over de identiteit ;

1. Morfologische verschillen

2. Morfologische overeenkomsten

3. Veel Morfologische vereenkomsten

4. Geen overtuigende conclusie



Toekomst Biometrie

Mobiele applicaties (politie gebruik)

Multi modal Biometrics (Synergie tussen modaliteiten)

Toename Artificial Intelligence

Toename deepfake en synthetische gezichten (i.e. deep fakes, morping and other counter measures to prevent recognition)

Big Data

Maatschappelijk gebruik

Betere data

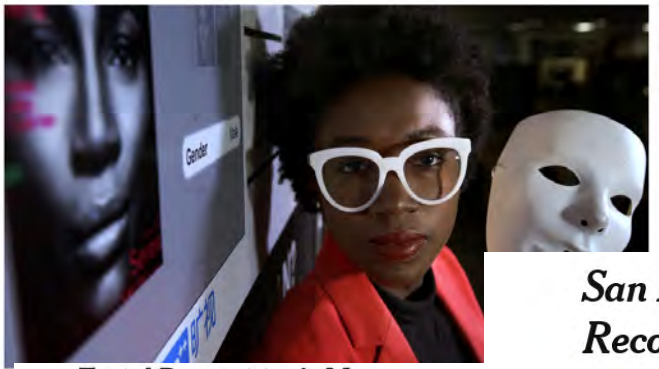
Onderzoek naar het creëren van betere data

- 9 afbeeldingen ipv 1 frontale foto
- Meer afdrukken van handpalmen
- Blote voet afdrukken
- Tattoos
- IRIS
- 3 D beeld van het lichaam?

AI experts take on Amazon after researcher's findings of racial bias in facial recognition

Published: Apr 3, 2019 4:57 p.m. ET

AI scholars call for Amazon to stop selling flawed software to police



Technology & Science · Analysis

Facial recognition is everywhere – here's why that's concerning

Whether the technology is being used for convenience or surveillance needs to be considered

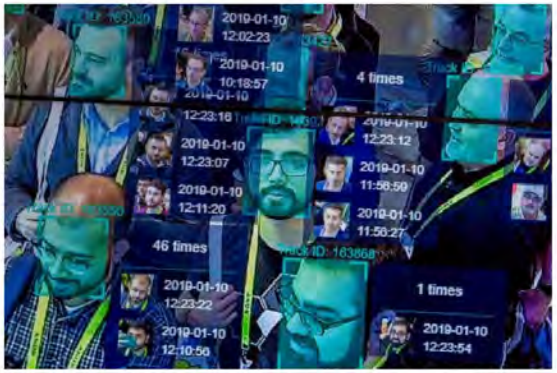
Ramona Pringle · CBC News · Posted: Sep 18, 2018 4:00 AM ET | Last Updated: September 18, 2018

Use of facial recognition tech 'dangerously irresponsible'

By Geoff White
BBC Click

13 May 2019 Share

Facial Recognition's Many Controversies, From Stadium Surveillance to Racist Software



The use of facial recognition technology in the public and private sectors has long been the subject of intense debate. David Mcnew/Agence France-Presse — Getty Images

San Francisco Bans Facial Recognition Technology

Attendees interacting with a facial recognition demonstration at this year's CES in Las Vegas.
Joe Buglewicz for The New York Times

INFOSEC TOPICS CERTIFICATIONS EVENTS CAREERS CONTRIBUTORS ABOUT INFOSEC

BIOMETRICS - PART 8

The Most Controversial Biometric of All – Facial Recognition

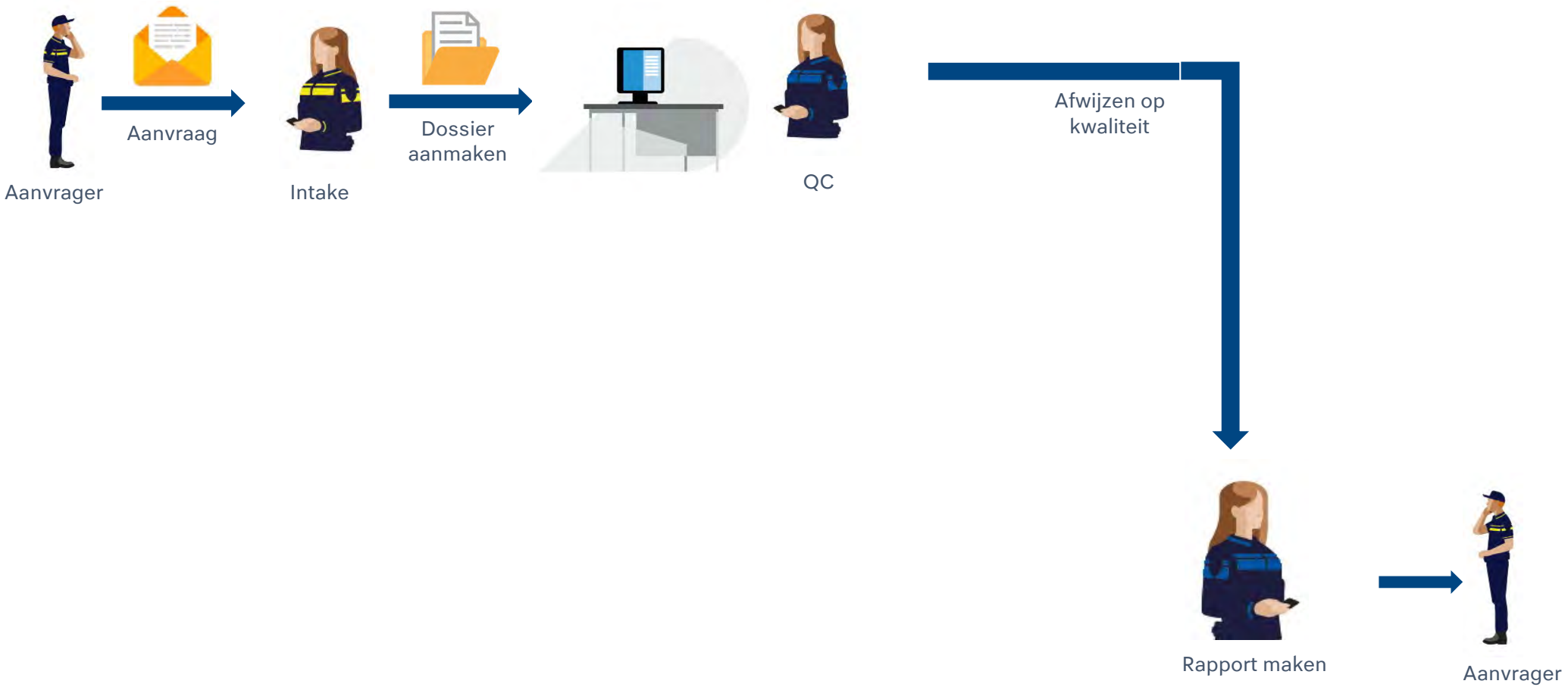
JUMP TO SELECT POST SECTION

Tweet Share reddit 1 Like

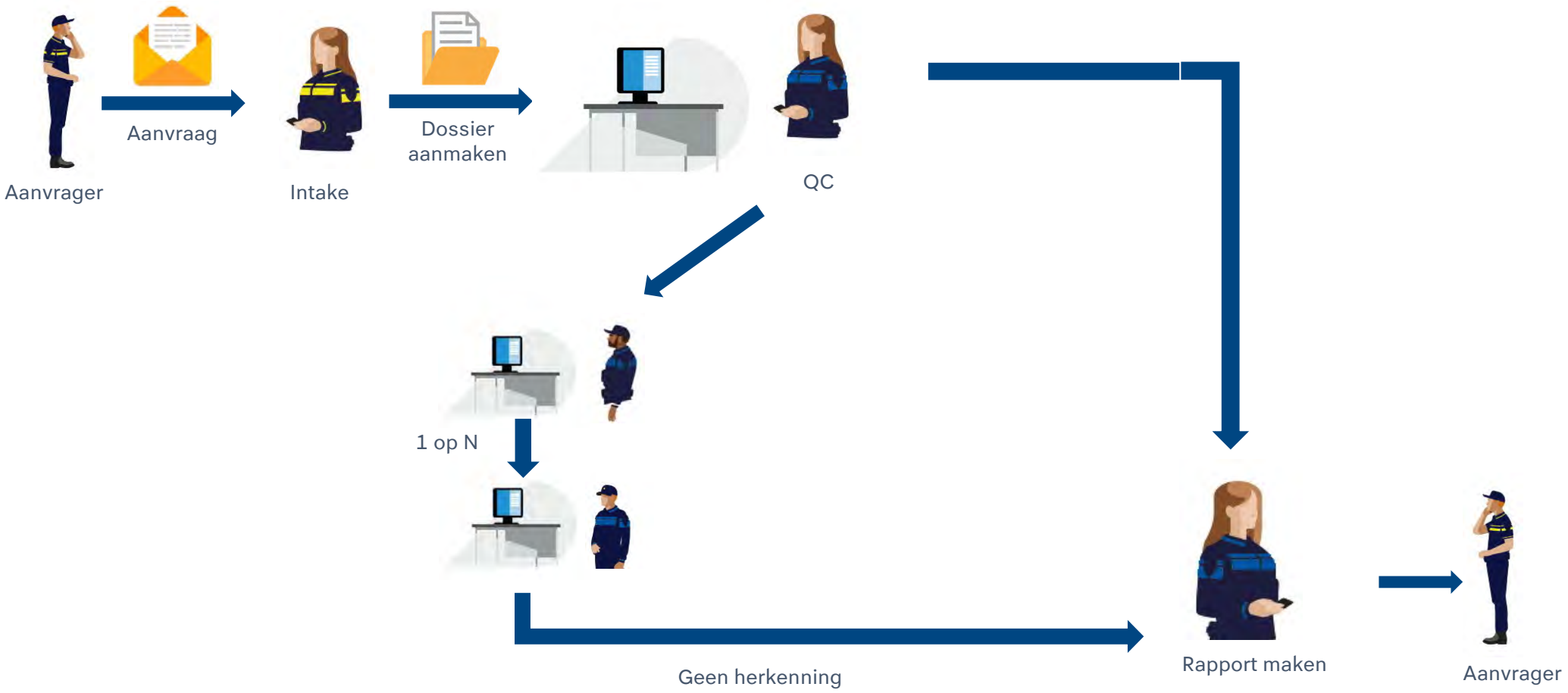
Vragen?

5.1.2.e [redacted]@politie.nl

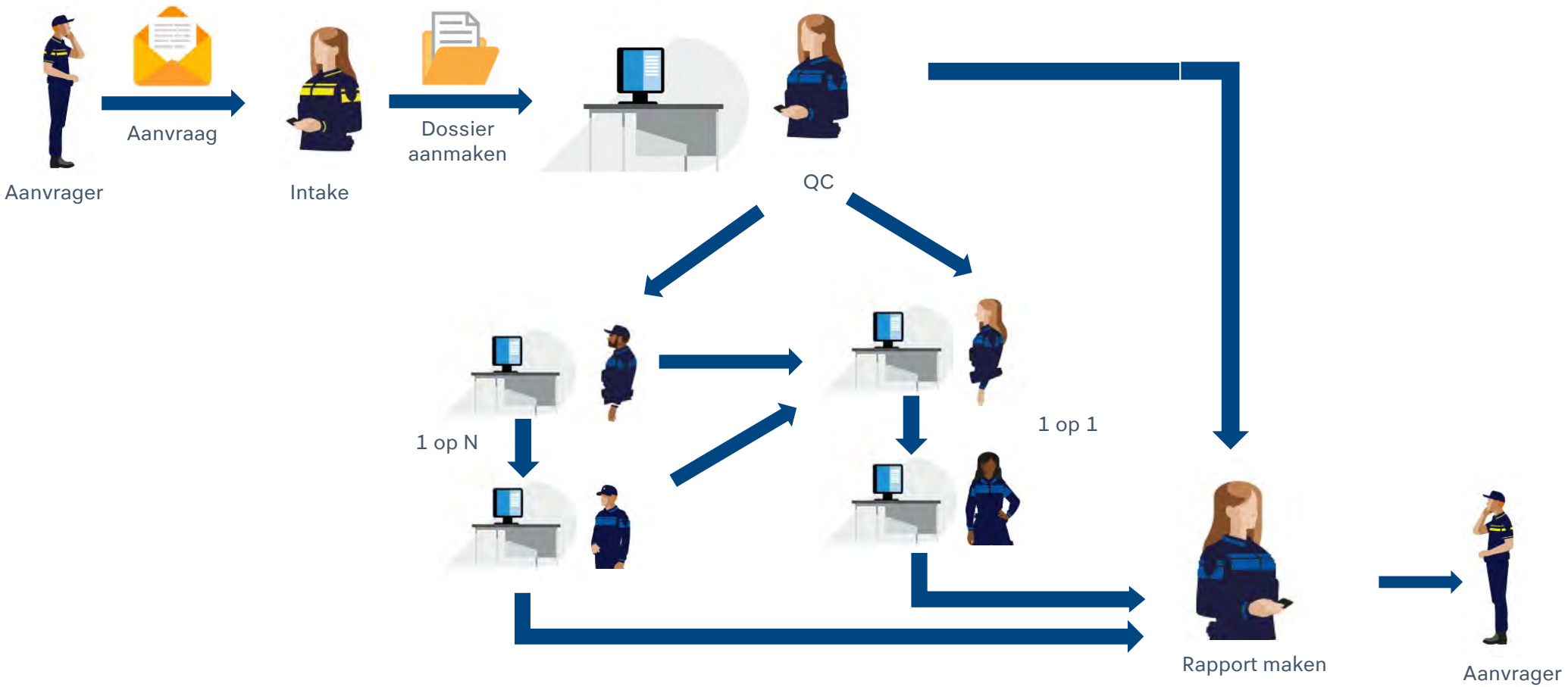
Proces gelaatsvergelijkend onderzoek



Proces gelaatsvergelijkend onderzoek



Proces gelaatsvergelijkend onderzoek



Use of Facial Recognition Technology for Law Enforcement Investigations

IDEMIA

How is facial recognition technology used for law enforcement investigations?

How does facial recognition work?

What does fairness in AI mean?

Introduction

Facial recognition technology (FRT) is becoming increasingly important to our ecosystems. It benefits a variety of sectors including public safety, law enforcement, and the commercial sector.

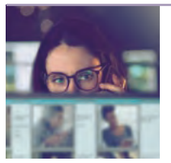
As with any emerging technology, its applications require discussions and debates based on the most factual and constructive elements possible with all stakeholders in society.

Face recognition

Face recognition is a software application that compares an image of a face against an image or database containing multiple images of faces. To conduct the comparison, FRT uses artificial intelligence (AI). Recent advances in AI have enhanced recognition capabilities and performance. It is important to note that modern AI techniques (i.e., deep learning) require a large amount of data during algorithm development to allow said algorithms to learn to recognize faces efficiently and unbiasedly.

Face recognition is used for various applications. Depending on a country's legislation, it may be used in the government or commercial sector:

Immigration border check



Investigation assistance in post-crime/ terrorist investigations

Creation and use of a digital identity, particularly for online public services

Facilitation of user authentication when using smartphone applications

This paper will focus on FRT's investigative use cases and IDEMIA's development and application for the law enforcement market.

1 How is facial recognition technology used for law enforcement investigations?

Boosting the efficiency of forensic examiners

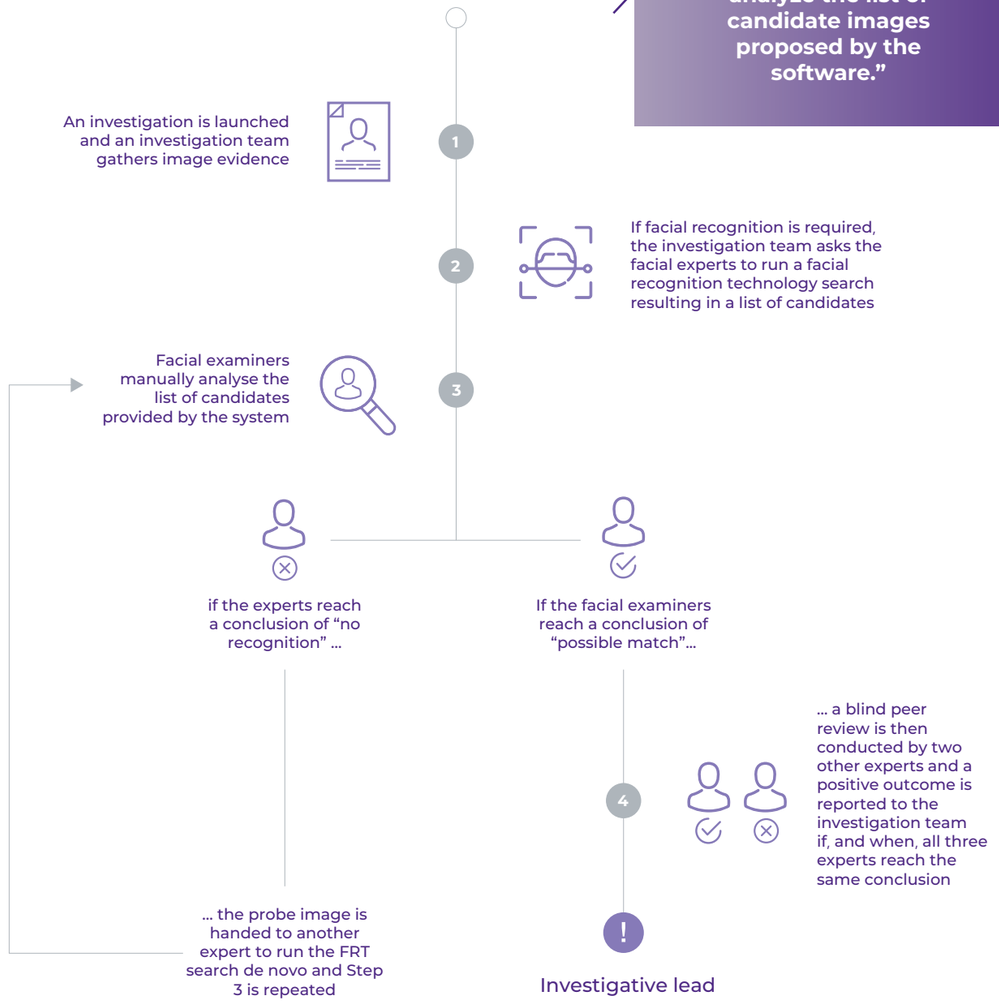
FRT is usually invoked when investigators have an image of the potential perpetrator's face, but have not been able to determine the person's identity. The FRT system compares this image to a database of faces of people known to the police. This database is typically composed of portraits (also known as 'mugshots') of people who have been, for example, previously arrested or involved in a criminal investigation for an offense serious enough to warrant the acquisition of biometric traits, including face, iris, fingerprints, palm prints, and DNA. If the system finds one or several faces similar to the searched face, then the system will propose a list of potential candidates for the forensic examiner to make an informed decision. If the system determines that no face in the database is similar enough to the searched face, then it will report that it found none.

Although, for the sake of its internal operation, the system produces a similarity score for every candidate, it is abundantly clear that this is still an estimation of probability, and that the final determiner is the trained human forensic examiner who will make a manual visual comparison of the two face images.

The system suggests potential candidates and the forensic examiner determines whether there is a possible match based on the standard operating procedures of the local police organization.

2 Use case: Netherlands Police uses a four-step process when using FRT

"After the search, facial examiners analyze the list of candidate images proposed by the software."



Source: The World Economic Forum's governance framework report for the responsible use of facial recognition in law enforcement investigations[1]

3 How does facial recognition work?

Algorithm development

Most characteristics of an FRT system are related to the algorithms used. For the sake of simplicity, we will focus on the biometric comparison algorithm. However, one must keep in mind that other factors play a key role, such as acquisition devices (e.g., cameras) and/or detection algorithms, which determine where the face is located in a photograph, or if there is an actual face in the photograph.

Most modern FRT approaches involve deep learning technology, which has been widely used for the last five to ten years, for many different applications, and is often referred to as 'Artificial Intelligence'. IDEMIA's FRT, like most other high performers, relies considerably on deep learning techniques.

In deep learning, the developer combines different elements to produce an algorithm:

- **Training dataset:** The developer puts together a dataset of known faces with different images of the same person, and many images of other people. This dataset allows the algorithm to 'learn statistically' what the commonalities are among a set of different pictures of the same person, and what the differences are among a set of pictures from different people.
- **Testing dataset:** This dataset is used to evaluate the performance of the algorithm. It is a completely different dataset to the training dataset but is labeled in terms of pictures of the same person or different people. This prevents over-adaptation of the algorithm to the training dataset, and enforces performance across a larger variety of operational situations.
- The **infamous 'cost function'** is a mathematical procedure by which the developer specifies which metrics they want the algorithm to optimize while learning. This procedure is not standardized. It is based on the developer's expertise, and objectives for the algorithm. In many ways, it is the 'secret ingredient' of an algorithm's performance.

Algorithm control and traceability

Once IDEMIA's algorithm has been trained, evaluated, and found compliant with the internal criteria, it can be used in operational systems. **After the algorithm has been released by R&D and is operational in IDEMIA's systems, it remains unchanged and its integrity remains intact throughout its lifecycle**. Existing products will be upgraded with a more recent version, which will also have been certified and released by our internal R&D department. IDEMIA does not use continuous learning or adaptation of an algorithm in production systems, i.e., in use by clients. In doing so, IDEMIA provides traceability, and guarantees the performance of our released algorithms which remain solely under our control. This is how IDEMIA assures clients and users that the performance of our algorithms is the same in the real world, as it was throughout testing.

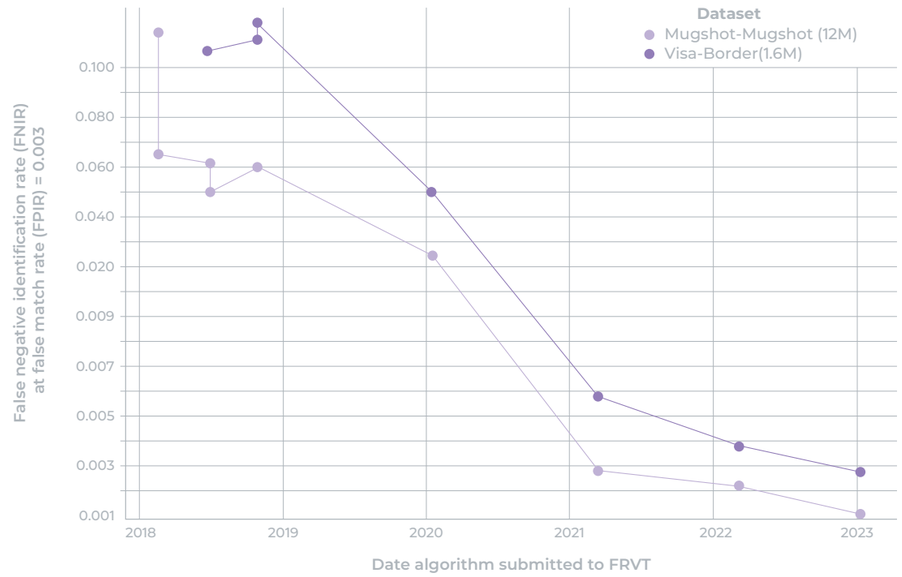
Relentless commitment to the improvement of technology

IDEMIA continuously invests in R&D and improves its state-of-the-art technology, be it algorithms, devices, or business processes. One key metric for this investment is the unremitting reduction of error rates of our FRT, as assessed by the independent organization, NIST[2], over a number of years.

Over the last three years, the accuracy of IDEMIA's algorithm improved by a factor of ten in a test that compares a picture against a database of pictures, as illustrated below.

Accuracy improved tenfold in the last three years.

Evolution of accuracy for IDEMIA algorithms on two datasets 2018 - present



Source: NIST FRVT 1:N Identification. NB: the lower the rate is the better the performance.

4 International working groups

To enhance transparency and ensure ethical use of FRT, IDEMIA is part of a number of working groups, and participates in developing industry standards. This allows IDEMIA to promote transparent communications about our technology.

Compliant with international standards pertaining to biometric technology

ISO/IEC 19795-1—Information Technology—Biometric performance testing and reporting

This standard defines methods and metrics to test the performance of biometric systems and algorithms through analysis of comparison scores and decisions output by the system, without requiring detailed knowledge of the system's algorithms or of the underlying distribution of biometric characteristics in the population of interest.

Industry associations

IDEMIA is an active member of several industry associations, such **Biometrics Institute** and **European Association** for Biometrics. IDEMIA frequently presents advances in biometric technologies to raise awareness about best practices and emerging technologies that help protect personal data in biometric applications[3]. We also facilitate discussions around fairness in biometric systems with major actors, including NIST and the UN Office on Counter Terrorism[4].

5 Compliance with stringent regulations

It is important to note that all of IDEMIA's research teams working on FRT algorithms are located in the EU (France and Germany), ensuring that the entire algorithm development process is compliant with GDPR, and, when the regulation comes into force, with the EU AI Act. Although at draft stage, the current text strongly emphasizes algorithmic fairness and responsibility of the developer—IDEMIA intends to fulfil these requirements in an exemplary manner.

GDPR compliance

Furthermore, IDEMIA is a long-standing partner of French administrative authorities and regularly collaborates with the CNIL (Commission Nationale de l'Informatique et des Libertés), through regular hearings and participations in consultations, including the pre-launch stage of an internal research program.

Strict proactive supervision of our research:

- IDEMIA is careful to respect strong ethical rules regarding data collection. Data is collected only for research purposes, in strict compliance with GDPR (i.e., on a voluntary basis, offering a right of access and rectification, and only for a limited period).
- Access to the data collected is strictly limited to our research staff, for a specific purpose and a specific period of time. The process that controls access to data has been certified ISO 27001 and is regularly audited.
- All of IDEMIA's intellectual property rights are protected in France and Germany and are therefore subject to the national regulations in force.
- IDEMIA felt it was essential to maintain our R&D laboratories in Europe, notably in France and Germany.

In addition, to address the ethical and technical issues raised by the lack of data, IDEMIA is working on the use of synthetic data for learning. In some cases, this data is necessary because it allows us to reach quite high recognition performances, especially on inanimate objects or optically read documents.

At this stage, state-of-the-art synthetic data does not provide convincing results for face images and thus does not correctly train facial recognition algorithms. IDEMIA is nevertheless actively working on improving this approach, which would solve the problem linked to the volume of data available.

Export control

In view of the risks associated with the deployment of facial recognition, it should be noted that for many years, IDEMIA's export control policy has referred to and complied with the most stringent international standards and guidelines, particularly in the area of human rights, such as the United Nations' guidelines. As a technology provider, it is IDEMIA's duty to comply with such standards and it is fundamental to have clients and partners who adhere to the same level of ethics.

6 What does fairness in AI mean?

Because FRT can be used in sensitive applications, such as criminal identification, it is important to make sure that when processing biometric data, the algorithm does not embed significant differences from the varying population categories. Even if, in the case of criminal identification, a human forensic examiner makes the final decision, it is crucial that the algorithm itself does not present error differentials.

The different categorization of the population can be considered; ethnic groups being one of the most prevalent, but also age, gender, whether or not the person is wearing glasses, has facial hair, facial accessories etc.

The most widely accepted definition of fairness in FRT is when systems present the same statistical performance across the different groups, so that the probability of error is not significantly different from one group to another. Of course, depending on the use case, an algorithmic error can have vastly different consequences for the person—from mild annoyance to a severe impact on fundamental rights.

False Positive Identification (FPI) happens when an FRT system erroneously presents one face as extremely similar to the searched face to the forensic examiner. This can potentially result in an individual being investigated even though they had nothing to do with the crime/incident. Although this can be cleared first and foremost by the expert decision of the face examiner, and later, by the investigative process, it is still an undesired outcome which shall bear the mark of statistical inequity. In the case of criminal identification, FPI is the type of error that needs to be limited, and stability across the different groups is necessary.

How does IDEMIA enforce fairness in AI?

IDEMIA applies cutting-edge techniques to the algorithm development process. The current public discourse on facial recognition and AI in general is that any disproportion in the training dataset (with underrepresented categories of population) will prevent fairness. The distribution of the training dataset is not the only factor influencing fairness. The cost function, and therefore, the expertise of the developer, will also have a significant impact on performance. By carefully building the training dataset and the cost function simultaneously, a developer can greatly influence the performance of the resulting algorithm.

The testing dataset must be:

- representative of the type of data that the algorithm will face in the field.
- representative of all population groups that the algorithm may face in the field.

A fairness assessment is an integral part of IDEMIA's algorithm development process.

This will ensure that the internal performance assessment reflects the behavior of the algorithm with fidelity.

Finally, IDEMIA selects algorithm candidates for release **not only based on pure identification accuracy, but also on fairness across the different population groups**.

All this would not carry much weight if it was limited to self-attestation and vendor claims.

Third-party testing for more transparency

IDEMIA submits its FRT algorithms (along with fingerprint and iris recognition technologies) to third-party testing organizations at every possible occasion. The most comprehensive testing series for FRT is NIST Face Recognition Vendor Test (FRVT)[5]. FRVT is an ongoing test, in the sense that any vendor can submit algorithms for testing (free of charge, so that company resources do not come into play here) and have the results published on NIST website, under NIST's care. All the datasets NIST uses for evaluation are the property of the US government. They are confidential, and sequestered so that no vendor has access to them, and therefore no alteration of the evaluation is possible.

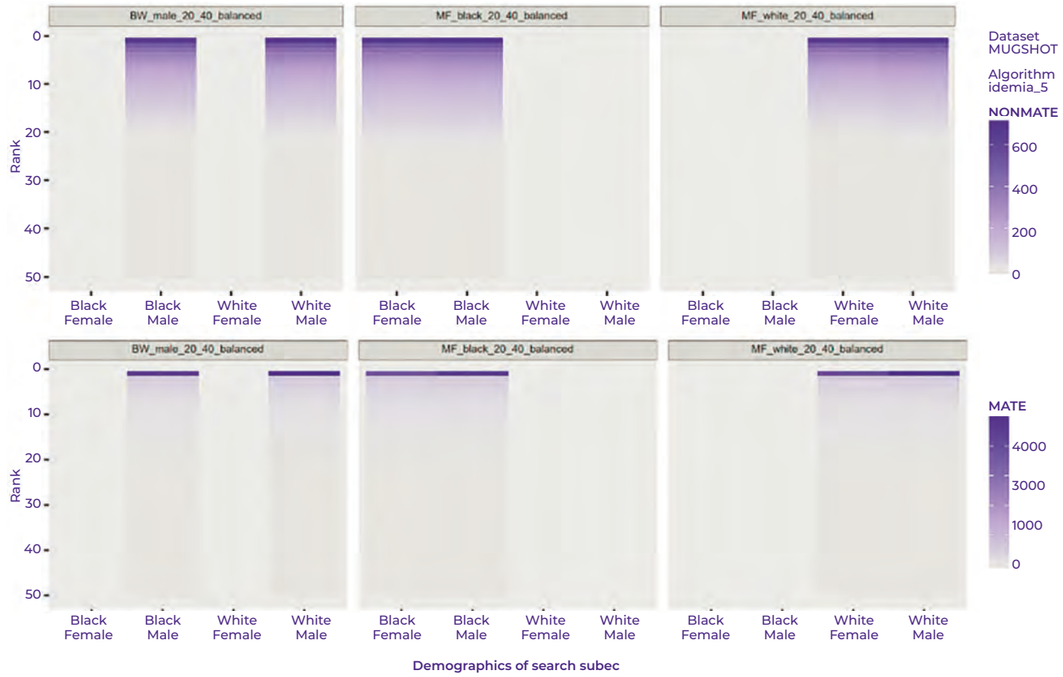
Focus on 'Demographic Effects'

NIST has been studying FRT 'Demographic Effects' very extensively and went as far as publishing a dedicated report[6] about it. Within this report, NIST studies error rates for a variety of vendor-submitted algorithms and reports performance in terms of fairness. The use case we are interested in is Criminal Identification, where consistency of the FPI rate across different population groups is the desired situation. On page 11 of the report, within the executive summary, in a section focusing on False Positive Error Rates of identification algorithms, the author writes:

It is noted that *"the presence of an enrollment database affords one-to-many algorithms a resource for mitigation of demographic effects that purely one-to-one verification systems do not have. We note that demographic differentials present in one-to-one verification algorithms are usually, but not always, present in one-to-many search algorithms.* ***One important exception is that some developers supplied identification algorithms for which false positive differentials are undetectable. Among those is IDEMIA, who publicly described how this was achieved"***[7].

Along with these statements, NIST published a range of statistics and technical results for IDEMIA's algorithms among many others. Currently, IDEMIA has submitted 402 algorithms by 114 unique developers that have been evaluated by NIST over the course of the FRVT program.

The figure below materializes the ability of IDEMIA's algorithms to maintain consistent performance over different ethnic groups, in the very specific use case of Criminal Identification (*performance measured on a mugshot dataset*):



Source: NIST FRVT Demographic Effects report, annex 17, figure 21

This graph illustrates that the IDEMIA algorithm processes all categories of people equally, regardless of their ethnic group or gender and serves as evidence of the statement of the executive summary of the report.

The shades of colors would be distributed very differently on the left (one demographic category) and on the right (same use case for a different demographic category), whereas they are uniform between all demographic categories for IDEMIA's algorithms.

The graphs show the distribution of 'rank' (how far a potential match is positioned in the list proposed to the forensic examiner) over different groups of people (skin tone variations and gender). The top graphs show the distribution of rank for 'non-mate' (not a match) and the bottom graph show the distribution of rank for 'mate' (exact match):

- The fact that the bottom graph shows most ranks to be zero, and a few below zero, is an indication that in the vast majority of cases, IDEMIA's algorithm proposed the correct match when it was present in the dataset.
- In the top graph, the fact that all shades of purple of the different bars are extremely similar illustrates that the algorithm performs very consistently across different groups.

7 Introducing measures for responsible facial recognition

The World Economic Forum, the International Criminal Police Organization (INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the Netherlands Police convened a multi-stakeholder community centered on co-designing a set of principles that outline what constitutes as the responsible use of FRT for law enforcement investigations. Among these principles is the respect for human and fundamental rights; human oversight and accountability; optimization of system performance and mitigation of error and bias.[8]

Assessing your technology provider for responsible facial recognition

These principles are accompanied by a self-assessment questionnaire to support law enforcement agencies with design policies surrounding the use of FRT and to ensure that the technology provider is in line with the proposed principles.

- What existing or forthcoming standards do you ask your vendor to follow to evaluate the performance of your FRT system?
- Have you introduced procurement rules to select providers who comply with these standards of performance?
- Have you introduced procurement rules to select providers who have submitted their FRT system to an independent evaluation such as that organized by NIST?
- Have you selected the technology provider who presented the best results?
- Are the independent lab tests of performance designed to model, as closely as possible, real-world objectives and conditions in which the FRT is applied?
- Do you notify the technology provider when you identify relevant errors in the use of the FRT system?
- What procurement rules have you introduced to ensure the regular upgrades or replacement of the FRT?

8 Testimonial from the Netherlands Police

"Preventing and solving crimes are two very important tasks, and therefore require the best technological support. The use of facial recognition technology has become essential for efficient policing since the volume of crime-related image and video data available has snowballed over the last few years. Less time spent on one investigation means more time to work on other important investigations and also to show due care to the victims of these crimes.

It is our responsibility to ensure that we choose a technology that has been created with the right ethics and values in mind from the outset. This technology must include the correct workflows that empower our investigators to pursue leads as quickly as possible, but also to ensure that human experts make the decision—every step of the way.

After a competitive tender, we found this technology, and it is provided by the market leader in biometric solutions—IDEMIA. IDEMIA develops its solutions on the following principles: fairness, inclusivity, efficiency and security regarding the uses, implementation and implications, both in public and private markets. We are proud to have IDEMIA on our side to create an even safer Netherlands."

John A.J.M Riemen

Lead Specialist on Biometrics
Center for Biometrics
Netherlands Police

Key takeaways

IDEMIA promotes technology improvement by participating in public, third-party evaluations, which show the transparency of technology capabilities through international standards.

FRT is used as a tool for investigators—decisions that may impact citizens' privacy and fundamental rights are always made by a human examiner.

IDEMIA's FRT is exclusively developed in Europe, and complies with all privacy standards and regulations including GDPR. Export Control applies to all our commercial activities inside and outside of Europe.

FRT is evolving quickly in terms of accuracy, resulting in error rates occurring five times less between 2018 and 2023.

Fairness is provided by design in IDEMIA's identification algorithms, as has been demonstrated by independent public evaluation of their performance by NIST.

Acknowledgments

We would like to thank our clients around the world, in particular the Netherlands Police, for the trust that they have placed in us over the years. Our joint collaboration enables us to reach the common goal of: making the world safer.

Furthermore, we would like to express a special thanks to the World Economic Forum, for the excellent report defining a framework for the safe and trustworthy use of facial recognition technology in law enforcement investigations. Six law enforcement agencies undertook an exercise to pilot the policy framework in order to review and validate its utility and completeness.

Endnotes

1 **The World Economic Forum:** A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations (Revised 2022).

WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (weforum.org)

2 The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the USA's oldest physical science laboratories.

3 **Biometrics Institute** Congress 2021 – October 13 2021, IDEMIA delivered a presentation entitled *How to enhance biometric applications to protect privacy?*

https://www.biometricsinstitute.org/event/biometrics-institute-congress-2021/

4 **EAB (European Association for Biometrics) Virtual Events Series** Demographic Fairness in Biometric Systems - March 2021 IDEMIA presented a lecture about *Fairness for Face Recognition* and participated in a panel discussion with major actors including NIST and the UN Office on Counter Terrorism.

https://eab.org/events/program/237

5 NIST Face Recognition Vendor Test.

https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

6 NIST Face Recognition Vendor Test, Part 3: Demographic Effects.

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

7 Stephane Gentric, IDEMIA's Head of Artificial Intelligence Research. Face recognition evaluation @IDEMIA. In Proc. International Face Performance Conference, National Institute of Standards and Technology NIST, Gaithersburg, MD, November 2018. Page 11,

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

8 Ongoing Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Annex 17: Candidate list score magnitudes by sex and race. Page 24, figure 21.

https://pages.nist.gov/frvt/reports/demographics/annexes/annex_17.pdf

About IDEMIA

With over 40 years' experience and over 5 billion records managed worldwide, IDEMIA is the undisputed leader in biometric systems. Our algorithms – consistently ranked in the top tier across many modalities and multibiometric solutions by NIST—combined with our product design and manufacturing expertise, make us the partner of choice for the most prestigious organizations.

We create off-the-shelf and tailor-made solutions to meet the complex and ever-changing demands of our customers. We supply biometric systems with IDEMIA's algorithms to law enforcement agencies around the world. We collaborate with the world's leading airports and airlines, providing them with compact solutions that use biometric technology to facilitate their day-to-day activities, bringing more security and peace of mind. We develop products and solutions in accordance with the Privacy by Design and by Default principles. We are strongly committed to helping protect and secure citizens' and consumers' privacy, with the highest possible level of data protection for identity verification and authentication technologies.

Our aim is to keep our world as safe and secure as possible, which is why we are dedicated to providing the most advanced tools and guidance available on the market.

For more information, visit **www.idemia.com**

Follow **@IdemiaGroup** on Twitter

Unlock the world, **make it safer.**

idemia.com/**market/public-security-identity**

IDEMIA

www.idemia.com

Facial Recognition/Comparison

POLITIE

John Riemen
2023

Facial recognition or facial comparison?

Facial Recognition

- *You have seen this person before.*
- *Recognise a person from your memory.*
- *Very powerful tool*
- *Also, easy to influence under stress or pressure*

Facial comparison

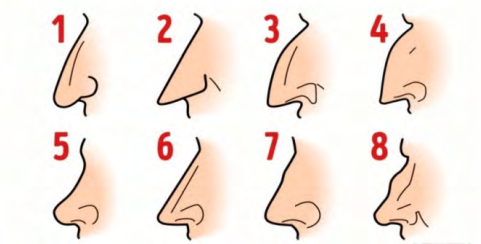
Facial comparison is a manual process conducted by a human which entails identifying similarities and dissimilarities between two (or more) images or an image and a live subject to determine whether they represent the same or different person.*

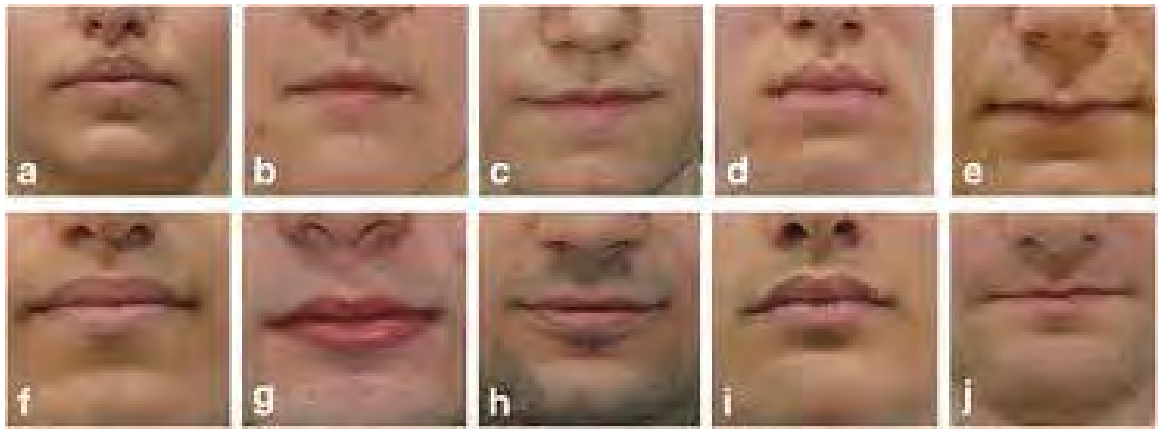
* https://fiswg.org/fiswg_facial_comparison_overview_and_methodology_guidelines_V2.0_2022.11.04.pdf

Facial comparison

Facial comparison method

- *There are three comparison methods (morphological analysis, superimposition, and photo-anthropometry) currently recognized in facial comparison.*
- *Morphological analysis is the direct comparison of class and individual facial characteristics without explicit measurement. It is the method of facial comparison in which the features and components of the face are compared.*
- *Morphological analysis (in some form) shall be the primary approach used for facial comparison in all categories: assessment, review, and examination. Observations in relation to similarity*





Facial recognition for Law Enforcement

Face comparison (since 2014) with a first generation Automated Face system (2015) to a ABIS from IDEMIA (2023)

- 1,5 million suspects and convicts
- 2,5 million face images

Criminal Law
“fingerprints and faces may be used for the prevention, detection, prosecution and sentencing of criminal acts”

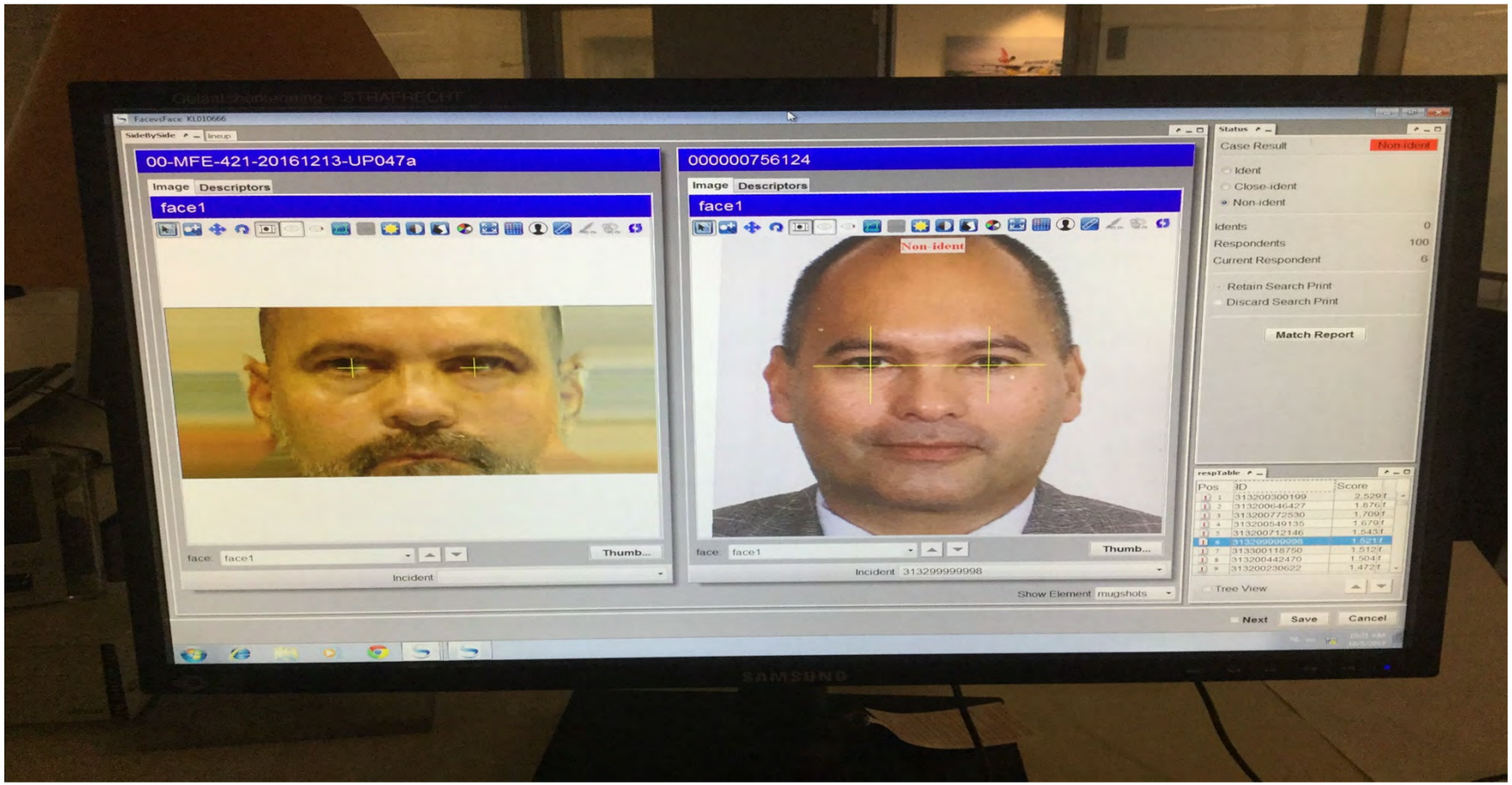
Between 1000-1500 facial comparisons for Law Enforcement purposes a year
Average HIT rate between 10-21 % (system 2015)

Also possibility to search alien database under Law with strict rules:

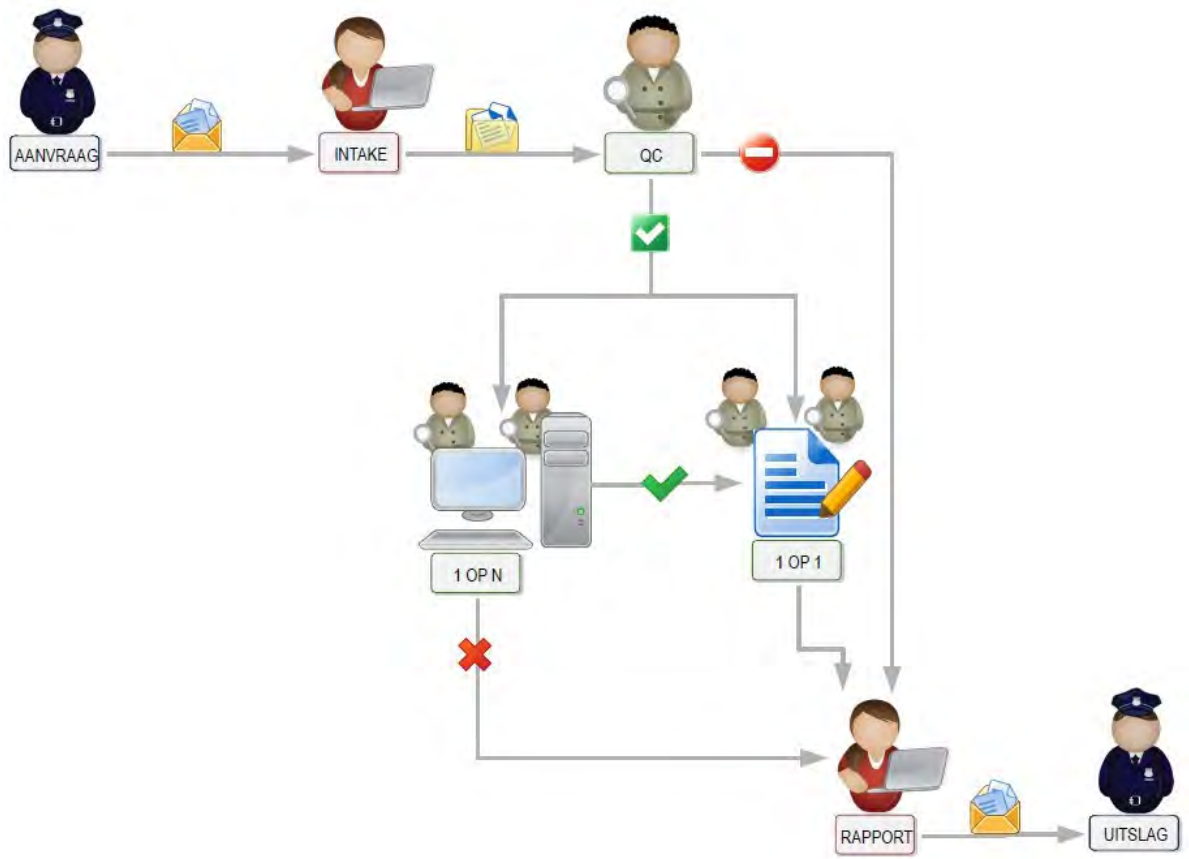
Alien law
- art 107 “ fingerprints and facial images maybe used for investigation and prosecution of criminal acts”.

Written order public prosecutor and authorised by an investigative judge

Facial Recognition System



Face comparison process



16

Full in-depth analysis after possible MATCH by 2 other experts

Results

In total 4 conclusions

- ***Many clues that face a and face b are <u>not of the same source</u>***
- ***<u>Clues</u> that face a and face b are of the <u>same source</u>***
- ***<u>Many clues</u> that face a and face b are of the <u>same source</u>***
- ***<u>Inconclusive</u> conclusion that face a and face b are of the same source***

Report to be used as a investigative lead!

DVI use Face

Pro's

- ***Huge amount of personal AM information available: phones/social media/pictures***
- ***Well documented reliable official AM information: passport/ID card***
- ***Huge governmental (visa) databases***
- ***Fast, simple relatively inexpensive***
- ***Facial Recognition systems highly accurate***

DVI use Face 2

Cons

- *Twins*
- *Family members can look very similar*
- *People (no family) can look very similar*
- *Mutilation of the face*
- *Photo Quality*

Javier Bardem Jeffrey Dean Morgan

John Riemen

06 5.1.2.e

5.1.2.e @politie.nl

Police of the Netherlands

1. Inleiding

Tussen 2016 en 2018 zijn er meerdere onderzoeken gestart in opdracht van DGRR voor het creëren van een gezamenlijk, door professionals en ketenpartijen gedeeld en gedragen beeld van de tekortkomingen die bestaan rond de toepassing van het wettelijke kader.

In 2019 heeft DGRR aan Justid gevraagd om een impactanalyse uit te voeren voor de knelpunten die voor Justid van toepassing zijn; bewaartermijnen, rechtspersonen en leidende administratieve identiteit.

Op basis van dit rapport is eind 2020 door DGRR opdracht gegeven aan Justid voor het uitvoeren van een door de keten ondersteunde business analyse plus advies met verbetervoorstellen en het opstellen van plan van aanpak voor deze drie knelpunten waar ketenpartners voor nodig zijn.

In februari 2021 is er vanuit DGRR een aanvullende opdracht aan de stuurgroep gegeven om vooruitlopend op de structurele oplossing voor het handhaven van de bewaartermijnen een eerste schoning uit te voeren van biometrische gegevens in de strafrechtketen.

In april 2021 is het rapport Analyse bewaartermijnen in de strafrechtketen opgeleverd en door de stuurgroep goedgekeurd.

Als gevolg van de maatschappelijke en politieke druk op het schonen van biometrische gegevens is in 2021 primair hieraan de aandacht besteed. Er is vanuit Justid een analyse gestart binnen SKDB naar de gegevens die geschoond moeten worden. Dit overzicht is door ketenpartners aangevuld en heeft geresulteerd in een eerste inzicht voor de schoningsstappen die nodig zijn.

2a. Behaalde resultaten tot nu toe: 2020- 2021

De oorspronkelijke opdracht van DGRR aan Justid: *'Hoe zaak en identiteitsvaststelling eenduidig gekoppeld kunnen worden en de Justitiële Informatiedienst haar rol als centrale bewaker van de bewaartermijnen binnen de strafrechtsketen kan invullen en aan haar verplichtingen op grond van artikel 5 Bivv kan voldoen'*

In april 2021 is het rapport Analyse Bewaartermijnen in de strafrechtketen opgeleverd.

Het rapport concludeert dat de problematieken in grofweg 3 aandachtsgebieden is weer te geven:

- Binnen de keten is niet altijd bekend welke biometrische gegevens bij welke persoon en welke zaak horen, zodat deze op de juiste momenten geschoond of vernietigd kunnen worden.
- Er wordt in de keten niet altijd gezorgd voor een trigger, waardoor bekend is wanneer zaak/biometrische gegevens/persoonsgegevens de bewaartermijnen in moeten (en wanneer ze geschoond en vernietigd moeten worden).
- Er vindt een selectieve registratie plaats van alleen documentabele en strafrechtelijke feiten in JDS, waardoor geen volledige bewaking van bewaartermijnen kan worden uitgevoerd.

Het rapport biedt input voor de volgende fase om deze punten met de ketenpartners te bespreken en oplossingsrichtingen uit te werken. Die oplossingsrichtingen geven input aan een plan van aanpak voor het daadwerkelijk realiseren van de oplossing in de keten.

2b. Behaalde resultaten tot nu toe: 2021 - 2022

In februari 2021 is vanuit het DGRR de opdracht voor dweilen van de wezen aan de stuurgroep gegeven:

- *80.000 bestaande wezen beoordelen en mogelijk biometrie vernietigen*
- *Eventuele aanvullende dweil acties door ketenpartners zelf worden opgepakt*

In de rest van het jaar 2021 is de matching van politie, OM en CJIB van de wezenlijst uit de SKDB tegen de basisadministraties uitgevoerd. De matching van de wezenlijst tegen de basisadministratie van de KMar is in april 2022 uitgevoerd.

De eerste analyses op de (deels) gematchte dataset zijn in januari 2021 reeds uitgevoerd door specialisten en vervolgens door het datascientisten-team.

Samenvatting van de inzichten uit de voorgaande fases:

- De analyse op basis van de matching biedt inzicht, maar verbanden zijn nog niet volledig in kaart gebracht
- De complexiteit is groter dan gedacht, dit zit hem in aantal betrokken ketenpartners, het aantal registraties die informatie bevatten die invloed hebben op de bewaartermijnen, omissies in wet- en regelgeving en in het werkproces bij de ketenpartners. Dit maakt dat het project een explorerend karakter heeft en elke plandatum van het opleveren van een resultaat alleen een inschatting kan zijn op basis van de huidige inzichten.
- Datakwaliteit start bij invoer en werkt door in de gehele keten, de schoningsaanpak en oplossingsrichtingen voor structurele oplossing moeten gezamenlijk opgepakt worden door de ketenpartners.

3. Bevindingen Bewaartermijnen & Dweilen

Overzicht bevindingen Bewaartermijnen

- Scope opdracht is beperkt tot bivv artikel 5. Gevraagd besluit stuurgroep op uitbreiding van de scope naar bivv 5, 6 en 7. Zonder deze uitbreiding is het voor Justid nog steeds niet mogelijk om de rol van centrale bewaker bewaartermijnen in de strafrechtketen in te vullen. De impact van deze (door de stuurgroep nog goed te keuren) scopeuitbreiding wordt meegenomen in de vervolgopdracht.
- Issues ontstaan grotendeels bij inschrijving en koppeling tussen processen identiteitsvaststelling (politie & KMar) en zaaksregistratie (OM/CJIB). Dit werkt door in de rest van de keten. Opdracht ombuigen naar ketenopdracht.
- Proces strafrechtketen wordt niet in alle gevallen doorlopen volgens procesflow (o.a. Halt). Daar waar procesverloop afwijkt (zoals buitenstrafrechterlijke afdoeningen) is nadere analyse van de procesinrichting nodig om te kijken of daar issues worden veroorzaakt en wat een mogelijke oplossingsrichting is. Deze oplossingsrichting kan zowel in aanpassing van wet- en regelgeving, aanpassing van werkprocessen als aanpassing van informatievoorziening liggen.

Overzicht bevindingen Dweilen

- Het huidige beeld is nog onvolledig en moet aangevuld worden met matching tegen andere basisadministraties zoals van Bijzondere Opsporingsdiensten en Rijksrecherche en de basisadministraties van potentiële systemen bij de huidige ketenpartners die nog niet zijn meegenomen in de huidige vergelijking.
- Aanvullende analyse is nodig om te bepalen of en zo ja welke schoningsstappen nodig zijn, hierbij zijn analyses vanuit alle processtappen van het strafrechtproces nodig om te komen tot categorieën van schoning.
- Huidige opdracht beperkt zich tot het schonen van registraties van biometrie uit de SKDB zonder zaaksgegevens op peildatum 1 januari 2021. Bewaartermijnen van registraties in SKDB waarbij persoonsgegevens en zaakgegevens niet eenduidig gekoppeld zijn, kunnen echter op dit moment ook niet gehandhaafd worden, een nadere schoningsstrategie is hiervoor noodzakelijk evenals voor de registraties van na 1 januari 2021. Deze schoningsstrategie beschrijft de aanpak van schoning van de data tot het moment dat de knelpunten in de informatievoorziening ketenbreed zijn opgelost en de bewaartermijnen (automatich) gehandhaafd kunnen worden.

4. Voorstel voor vervolgstappen bewaartermijnen & dweilen

2022 – e.v.

Bewaartermijnen (structurele oplossing)

- Bijgestelde opdrachtbeschrijving die rekening houdt met de bevindingen uit de eerdere fase
- Nadere analyse om te bepalen of en welke schoningsstapepen nodig zijn op basis van de huidige opdracht
- Faseplan voor vervolgfase

Dweilen

- Aanvullen van de matching op basis van bevindingen uit vorige fase (onvolledig beeld door ontbreken van informatie)
- Nadere analyse om te bepalen of- en welke schoningsstappen nodig zijn op basis van huidige opdracht
- Komen tot categorieën voor schoning en advies aan stuurgroep
- Het maken van een schoningsstrategie voor een actuele gegevensset in de strafrechtketen tot het moment dat de oplossingen voor de knelpunten in de informatievoorziening ketenbreed zijn gerealiseerd.

HWt(8

5. Status en bevindingen LAI en Rechtspersonen

Leidende administratieve Identiteit

- Opdracht gegeven aan Justid, lijkt ketenopdracht
- Aan PL’s vragen om te bekijken of hiervoor bijstellen van de opdracht nodig is

NHR

- Opdracht gegeven aan Justid, vooralsnog Justid interne analyse
- Op een later moment besluiten of dit binnen de stuurgroep gebracht moet worden

Dia 6

HWt(8 in afwachting van business consultant on hold allemaal. Slide verstoppen

5.1.2.e (Justid); 18-5-2022

6.1 Dweilen van wezen

Projectdoel:

Op korte termijn zorgdragen dat schoning plaatsvindt van biometrische gegevens in de strafrechtketen van wezen (persoonsregistraties in de SKDB zonder zaaksverwijzing op peildatum 1 januari 2021) welke conform bivv art 5 reeds geschoond hadden moeten worden.

Projectresultaat:

1a. Vastgestelde schoningsstappen op basis van huidige opdracht

1b. Categorieën voor schoning en advies aan stuurgroep

1c. Schoning van de gegevens in de strafrechtketen op basis van de categorieën en het advies

1d. Het maken van een strategie voor schoning voor een actuele gegevensset in de strafrechtketen

6.2 Bewaartermijnen - structureel

Projectdoel:

De burger kan erop vertrouwen dat biometrische gegevens die zijn afgenomen in het kader van een identiteitsvaststelling conform geldende wet en regelgeving worden beheerd en verwerkt door de daartoe bevoegde organisaties in de strafrechtketen.

Projectresultaat:

1a. Ketenbrede businessanalyse van de omissies bij de verwerking van identiteitsgegevens verdachten en veroordeelden conform Bivv bij de organisaties in de strafrechtketen

1b. Ketenbrede inventarisatie van oplossingsrichtingen met hierbij een advies

1c. Plan van aanpak voor realisatie van uiteindelijke oplossingen op het gebied van wet- en regelgeving, beleid, werkproces, en informatievoorziening

Actie NR	KJ	Rapport Maatregel Uit KJ analyse	Categorie Maatregel	Afk	Rapport NR	Rapport Aanbeveling / Bevinding	Rapport Toelichting	Management Response Beantwoording vanuit KJ	Rapport Domein	Update Kans	Update Impact	Update Risico	Update Complexiteit	Update Risico mitigatie	Bron Aanbeveling of Techn. Maatregel	Termijn oplossing (Gepland)	Status	Voorstel Oplossende partij (Generiek)	Voorstel Oplossende partij (Detail)	Opmerkingen
892	Biometrievoorziening	Personaliseer het DevOps account	Verbeter autorisatie(s)	BIV4	2.2	Beperkt beheer toegangsrechten DevOps account	Zorg dat het DevOps account niet voor elke beheerder toegankelijk is, en dat inloggen alleen kan via een persoonlijk beheerderaccount voor elke beheerder. Gebruik bij voorkeur een tweede authenticatie factor (2FA).	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC04 Controlled Use of Administrative Privileges	L	H	M	M	M	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**15-3-2022** Aangezien PAM niet op de GI gerealiseerd gaat worden, gaat het team zelf (samen met Atos) gepersonaliseerde beheeraccounts aanmaken met Sudo rechten. Dit gebeurt voor live-gang. **16-07-2021** Is dit niet iets dat platform breed opgelost moet worden? **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
893	Biometrievoorziening	Periodieke KeePass wachtwoordwijziging	Verbeter autorisatie(s)	BIV5	2.3	Beperkt beheer toegangsrechten DevOps account	Wijzig het KeePass wachtwoord periodiek, bij voorkeur jaarlijks.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC04 Controlled Use of Administrative Privileges	L	H	M	L	M	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**21-3-2022** check core team of wij dit inmiddels doen. **16-07-2021** Is dit niet iets dat platform breed opgelost moet worden? **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
896	Biometrievoorziening	Implementeer herstelmogelijkheden voor individuele bestanden op de database	Implementeer een generieke voorziening voor back-up	BIV8	3.2	Ontoereikend back-upbeleid	Implementeer een methode waarbij niet alleen het hele platform maar ook individuele bestanden hersteld kunnen worden na een mogelijke gebruikersfout of aanval op de database.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC10 Data Recovery Capabilities	L	H	M	L	M	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**26-7-2022** Naast dat we de dagelijkse infrastructurele backup van Oracle PaaS gebruik kunnen maken in geval van nood, heeft het InfraBedrijf ook besloten tot de aanschaf van een off-line backup voor Oracle PaaS databases die teams zelf kunnen bedienen. De verwachting is dat we Q4 2022 hiervan gebruik kunnen maken. **15-3-2022** Oracle PaaS heeft niet de beschikking over een data back up systeem dat de klant kan bedienen. Om de eisen van de business, de formele accreditatie, te kunnen voldoen zijn wij met Oracle PaaS overeengekomen voor de Biometrievoorziening in geval van nood tijdelijk (tot de invulling van het changeverzoek) gebruik te maken van de infrastructurele back-up van PL Oracle Linux. Er is een change ingediend om op de lange termijn deze backup zelf te kunnen maken. Echter totdat finanicering geregeld is kan Oracle Linux dit niet aanschaffen. Verzoek ligt bij hoofd Infrabedrijf. Hij is op zoek naar financiering. **16-07-2021** We zijn hiermee bezig in het kader van de continuiteit van de voorziening en haar data. Biomen-5391, 5392, 5432, 5433, 5336 en 5589. Zie opzet memo Oplossen voor oor live-gang **01-04-2021 Sector IB - Beleid:** - Operationalisering door eigenaar van data. Door aan te geven hoeveel data verliezen. - Minimaal 1x per jaar restore, back-up toetsen op volledigheid. - Vervolgactie n.a.v. .
897	Biometrievoorziening	Verifieer de back-ups	Verifieer back-up	BIV9	3.3	Ontoereikend back-upbeleid	Laat de back-up software de integriteit van de back-up verifiëren en voer periodiek controles uit om de herstelfunctie van de back-ups te kunnen garanderen.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:** Biometrievoorziening zal op basis van het beleid rondom back-ups de back-up verifieren en afspraken (SLA/OLA) maken met het Infrabedrijf over de wijze van het maken van back-ups.	CSC10 Data Recovery Capabilities	L	H	M	L	M	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**26-7-2022** Naast dat we de dagelijkse infrastructurele backup van Oracle PaaS gebruik kunnen maken in geval van nood, heeft het InfraBedrijf ook besloten tot de aanschaf van een off-line backup voor Oracle PaaS databases die teams zelf kunnen bedienen. De verwachting is dat we Q4 2022 hiervan gebruik kunnen maken. **15-3-2022** Oracle PaaS heeft niet de beschikking over een data back up systeem dat de klant kan bedienen. Om de eisen van de business, de formele accreditatie, te kunnen voldoen zijn wij met Oracle PaaS overeengekomen voor de Biometrievoorziening in geval van nood tijdelijk (tot de invulling van het changeverzoek) gebruik te maken van de infrastructurele back-up van PL Oracle Linux. Er is een change ingediend om op de lange termijn deze backup zelf te kunnen maken. Echter totdat finanicering geregeld is kan Oracle Linux dit niet aanschaffen. Verzoek ligt bij hoofd Infrabedrijf. Hij is op zoek naar financiering. **26-07-2021:** **Toevoeging:** Ook het maken van afspraken (SLA/OLA) met het Infrabedrijf maken onderdeel uit van de validatie actie. **16-07-2021** We zijn hiermee bezig in het kader van de continuiteit van de voorziening en haar data. Biomen-5391, 5392, 5432, 5433, 5336 en 5589. Zie opzet memo Oplossen voor oor live-gang

898	Biometrievoorziening	Verhoog de reguliere patchfrequentie	Implementeer of verbeter het patch/upgrade proces of voer de acties rondom patchen en upgrades door	BIV10	4.1	Patches worden niet snel genoeg geïnstalleerd	Update de applicaties vaker met de nieuwste stabiele versies die de security updates omvatten, met name bij onopgeloste NCSC High-High security kwetsbaarheden die van toepassing zijn op de applicaties. De aangeraden patchfrequentie en de richtlijn vanuit het patchproces binnen de Nationale Politie is één keer per vier weken. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd. Houd versie-informatie van software bij, idealiter in een CMDB.	**Huidige stand van zaken / beantwoording:** Het Biomen-team is bezig dit in te regelen. **Vervolgactie:** Biometrievoorziening zal het patch management beleid en de bijbehorende procedures volgen.	CSC03 Continuous Vulnerability Assessment and Remediation	L	H	M	L	M	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**15-3-2022**5. High-High patches voor GI en Oracle PaaS worden gewoon conform NP beleid direct doorgevoerd door Infraberijf. Met betrekking tot versachillende prio patches zijn met leverancier IDEMIA in SLA en DAP afspraken gemaakt. **16-07-2021**5. Check bij Ing Lim applicatiemanager, hoe hij dit heeft ingeregeld in SLA en DAP 2.e Oplossen voor live-gang
899	Biometrievoorziening	Formaliseer een spoed patchprocedure	Implementeer of verbeter het patch/upgrade proces of voer de acties rondom patchen en upgrades door	BIV11	4.2	Patches worden niet snel genoeg geïnstalleerd	Formaliseer een spoed patchprocedure, zodat gegarandeerd wordt dat kritische kwetsbaarheden worden gedicht met een snellere doorlooptijd dan in het reguliere patchproces. De richtlijn voor de maximale doorlooptijd hiervan vanuit het proces binnen de Nationale Politie is 72 uur. Zorg ervoor dat de rol die de beheerder verantwoordelijk voor HHS patches inneemt goed wordt overgedragen als deze beheerder het team verlaat.	**Huidige stand van zaken / beantwoording:** Het Biomen-team is bezig dit in te regelen. **Vervolgactie:** Biometrievoorziening zal het patch management beleid en de bijbehorende procedures volgen.	CSC03 Continuous Vulnerability Assessment and Remediation	L	H	M	L	L	Observaties interviews	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**15-3-2022**5. High-High patches voor GI en Oracle PaaS worden gewoon conform NP beleid direct doorgevoerd door Infraberijf. Met betrekking tot versachillende prio patches zijn met leverancier IDEMIA in SLA en DAP afspraken gemaakt. **16-07-2021**5. Check bij Ing Lim applicatiemanager, hoe hij dit heeft ingeregeld in SLA en DAP 2.e Oplossen voor oor live-gang
901	Biometrievoorziening	Beperk EPB-communicatie d.m.v. een allow-list	EPB verbetering	BIV13	5.2	Onveilige dataoverdracht via de EPB	Sta op de Biometrievoorziening alleen communicatie toe van en naar IP-adressen van de communicerende servers van de EPB (het EEP). Dit kan bijvoorbeeld met host-based firewalls worden afgedwongen. Sta op EEP servers alleen communicatie toe van en naar IP-adressen van diensten die via de EPB informatie dienen uit te wisselen.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:** De aanbeveling zal worden voorgelegd aan het Productiehuis - EPB team.	CSC12 Boundary Defense	L	H	M	L	L	Observaties interviews	Nader te bepalen	Aansluiten op roadmap van generieke voorziening	KJ	KJ Biometrievoorziening	**21-3-2022:** Status opgevraagd5.1.2.e **20-05-2021:** Acties bijgewerkt in: 5.1.2.i **12-04-2021:** Bevinding voorgelegd met andere EPB bevindingen aan het EPB team.
902	Biometrievoorziening	Versleutel de data	Implementeer data versleuteling	BIV14a	6.1	Onversleutelde dataopslag	We raden aan om de data op de database te versleutelen (encrypten), zodat een aanvaller, wanneer hij toegang heeft tot het systeem, niet direct alles kan uitlezen. Daarnaast raden we aan om data op de back-uplocatie te versleutelen. Uit gesprekken met het Oracle PaaS team is gebleken dat er al een product zo goed als klaar ligt om in gebruik te worden genomen, maar dit is nog niet is gebeurd.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC13 Data Protection	L	H	M	M	M	Observaties interviews	31-12-2022	In uitvoering: Lange termijn	KJ	KJ Biometrievoorziening	**20-08-2021**5.1.2.e Op het platform zijn we met het confi project gestart om security op een hoger nivo te krijgen.Twee onderdelen zijn: Encryptie van de database, daarmee is ook de (infrastructuur) backup versleuteld. We moeten nog een aantal rollen beleggen waarmee we KeyManagement niet bij de leverancier beleggen, maar binnen een aangewezen afdeling, gemandateerde van de politie. Andere is het afschermen van de gebruikers data binnen de database zodat leverancier en beheerder geen rechten hebben of krijgen om deze data in te zien. De beheerders en leverancier moeten nog wel rechten hebben om patch en live cycle management uit te kunnen voeren. Fijnmazige rechten. Ook hier moet naast de techniek ook in het proces voorkomen worden dat "de slager zijn eigen vlees keurt". Hier moeten ook rollen en rechten gedefinieerd worden. Techniek van Oracle: - KeyVault (encryptie) - DatabaseVault (fijnamzige rechten data toegang) Implementatie op het Oracle Platform waarschijnlijk dit jaar, begin volgend jaar. Voor oplossingen binnen conventioneel zie ik het nog niet. **26-07-2021:** Deloitte werkt een PVA uit.
903	Biometrievoorziening	Versleutel mobiele gegevensdragers	Versleuteling van mobiele gegevensdragers	BIV15	7.1	Geen beleid voor versleutelen van mobiele gegevensdragers	Dwing versleuteling af bij het gebruiken van mobiele gegevensdragers. Blokkeer mobiele gegevensdragers volledig (op de VMs) wanneer deze niet nodig zijn voor de werkzaamheden.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:** Biometrievoorziening maakt geen gebruik van USBsticks. Dit is ook gecommuniceerd naar stakeholders.	CSC13 Data Protection	L	H	M	M	M	Observaties interviews	Gereed	Uitgevoerd	KJ	KJ Biometrievoorziening	**05-07-2021 Update met Biometrievoorziening:** **Gereed.** Biometrievoorziening maakt geen gebruik van USBsticks. Dit is ook gecommuniceerd naar stakeholders. **12-04-2021:** Generieke aanbeveling, er zal via Awareness aandacht voor gevraagd worden https://intranet.politie.local/vraagenantwoord/1206/ict-middelen---usb-sticks.html **25-03-2021:** Aanbeveling voorleggen aan Sector IB - Beleid, afstemmen met o.a.5.1.2.e Deze aanbeveling komt bij vrijwel ieder KJ terug.
912	Biometrievoorziening	Stel restricties in op data-activiteit	Implementeer of verbeter security monitoring	BIV24	11.1	Geen restricties op ongebruikelijke data-activiteit	Stel restricties in op ongebruikelijke data-activiteit zoals bijvoorbeeld het overmatig openen, bewerken, verwijderen, downloaden en uploaden van data zoals vinger- en gelaatsafdrukken, alvorens het account (tijdelijk) te blokkeren. Bekijk hierbij vanuit functioneel beheer of er uitzonderingen nodig zijn zodat essentiële processen niet onnodig worden belemmerd.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC16 Account Monitoring and Control	L	M	L	M	L	Observaties interviews	Nader te bepalen	In uitvoering	KJ	KJ Biometrievoorziening	**26-7-2022:** Aansluitprocedure voor LAAS en SOC lopen. Alle koppelingen zijn al op LAAS aangesloten. Dat geldt ook voor GI en Oracle PaaS als geheel (waar de Biometrievoorziening op staat). **21-3-2022:** Wij krijgen maar moeizaam contact met SOC en LAAS. Aangezien wij onze eigen monitoring en logging al hebben ingericht, pakken we dit na go-live op. **06-07-2021 SOC -**5.1.2.e Restricites zijn domein van Eigenaar / PO niet vanuit CSP of IB. **15-04-2021 SOC -**5.1.2.e Actie eigenaar: KJ Categorie oplossing: Beleid Beleid bepalen. **09-04-2021:** Bekijken mogelijkheden vanuit applicatie, los van monitoring activiteiten.

913	Biometrievoorziening	Inventariseer alle gevoelige data binnen de omgeving	Implementeren data classificatiemodel	BIV25	12.1	Onvolledig dataclassificatie model	Inventariseer waar alle data zich bevindt binnen de omgeving van de Biometrievoorziening en zorg dat er een overzicht gedocumenteerd is.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC13 Data Protection	M	L	L	L	L	Observaties interviews	Nader te bepalen	In uitvoering: Korte termijn	KJ	KJ Biometrievoorziening	**21-3-2022 en 16-07-2021** Check bij 5.1.2.e wie dit moet organiseren binnen Biometrie
914	Biometrievoorziening	Stel een dataclassificatiemodel op	Implementeren data classificatiemodel	BIV26	12.2	Onvolledig dataclassificatie model	Breidt de classificatie op geïnventariseerde data op gevoeligheid uit, gebaseerd op de wettelijke eisen en geschatte impact bij aanpassing, diefstal of vernietiging, en documenteer deze. Zorg dat gepaste beveiligingsmaatregelen worden toegepast per gevoeligheidsniveau. Zorg door middel van processen dat het data classificatiemodel up to date blijft, bijvoorbeeld door middel van jaarlijkse evaluaties of bij het toevoegen van nieuwe processen aan de Biometrievoorziening omgeving.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC13 Data Protection	M	L	L	M	L	Observaties interviews	Nader te bepalen	In uitvoering: Korte termijn	KJ	KJ Biometrievoorziening	**21-3-2022 en 16-07-2021** Check bij 5.1.2.e wie dit moet organiseren binnen Biometrie
915	Biometrievoorziening	Beperk toegang tot de NFS shares	Verbeter autorisatie(s)	BIV27	13.1	Openbare NFS shares beschikbaar op het interne netwerk	We adviseren om de configuratie van de NFS mounts aan te passen, zodat ze alleen bereikbaar zijn voor geautoriseerde gebruikers.	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	M	H	H	L	H	Observaties interne infrastructuur test	Nader te bepalen	Uitgevoerd	KJ	KJ Biometrievoorziening	**15-3-2022** Dit is inmiddels opgelost en ticket gesloten. **16-07-2021** Het Biomen-team is met de leverancier in overleg hoe dit op te lossen. Oplossen voor live-gang. **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
916	Biometrievoorziening	Beperk toegang tot de beheerinterfaces	Beperk toegang tot beheerinterfaces	BIV28	14.1	Beheerinterfaces beschikbaar op het interne netwerk	We raden aan beheerwerkzaamheden uit te voeren via een ander kanaal dan die van normale gebruikers naar de servers. Het is mogelijk om IP filtering te gebruiken om toegang tot de beheerinterface te limiteren tot specifieke locaties of systemen, maar in het geval van de Politie zouden beheerservices alleen beschikbaar moeten zijn vanaf het iscbeheer.local netwerk via de beheer netwerkinterface op de systemen; Daarnaast raden we aan om HTTP te vervangen door de veiligere variant HTTPS die over een versleutelde verbinding communiceert; Tot slot raden we aan om authenticatie af te dwingen op iedere beheerinterface met een tweede authenticatie-factor (MFA/2FA). Kies bij het implementeren van MFA/2FA voor een 'two-factor' authenticatie oplossing welke gebaseerd is op 'standards-based' algoritmen en authenticatie protocollen (zoals de Google Authenticator of het U2F-protocol).	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	L	H	M	L	M	Observaties interne infrastructuur test	Nader te bepalen	Won't fix	KJ	KJ Biometrievoorziening	**26-7-2022:** Ticket is gesloten en we gaan dit niet doen (zie ticket). **21-3-2022:** Vraag uitgezet in team. **16-07-2021** Het Biomen-team is met de leverancier in overleg hoe dit op te lossen Oplossen voor live-gang.
917	Biometrievoorziening	Verbeter de SMB configuratie	Connectie verbetering	BIV29	15.1	Onveilige SMB configuratie	Wij raden aan om gebruik te maken van "SMB Signing". Door deze optie te gebruiken worden de SMB pakketten op netwerk niveau beveiligd met een digitale handtekening. Hierdoor kan de ontvanger van het bestand altijd de authenticiteit en integriteit van het bestand valideren.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	L	M	L	L	L	Observaties interne infrastructuur test	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**15-3-2022** Is dit iets wat wij als Biometrie applicatie wel kunnen oplossen?
918	Biometrievoorziening	Schakel cleartext authenticatie uit	Connectie verbetering	BIV30	16.1	Gevoelige data onversleuteld verstuurd	Schakel cleartext authenticatie uit in de configuratie van de AMQP services.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	L	M	L	L	L	Observaties interne infrastructuur test	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**15-3-2022** Is dit iets wat wij als Biometrie applicatie wel kunnen oplossen?
919	Biometrievoorziening	Verbeter de SSL/TLS configuratie	Connectie verbetering	BIV31	17.1	Onveilige SSL/TLS configuratie	We raden aan de TLS configuratie op de kwetsbare systemen te verbeteren. Dit kan gedaan worden door: Een unieke 2048-bit of sterkere Diffie-Hellman Group te gebruiken; TLS 1.2/1.3 met GCM te ondersteunen; Alleen ondersteuning te bieden voor sterke cipher algoritmen met een minimale sleutellengte van 128 bits en die geen gebruik maken van het MD5 algoritme; Te onderzoeken of TLS 1.0 en TLS 1.1 nodig zijn voor de huidige gebruikers van de applicatie. Indien mogelijk raden wij aan TLS 1.0 en 1.1 uit te schakelen. Zie ook: https://www.ssllabs.com/projects/best-practices/index.html voor een gedetailleerde aanpak om TLS op een veilige manier te configureren	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	L	M	L	L	L	Observaties interne infrastructuur test	31-12-2021	Uitgevoerd	KJ	KJ Biometrievoorziening	**26-7-2022:** Onderstaande tickets zijn gesloten en uitgevoerd. Al het verkeer is TLS1.2 TLS1.3 is pas beschikbaar vanaf RHEL8. Wordt op zijn vroegst Q4 2022. **30-07-2021:** **Status:** ? resterend. **Via:** https://agora.portal.politie.local/sites/210622092424/SitePages/Start.aspx **16-07-2021** 1 jira item opgelost, 2e nog op te lossen

920	Biometrievoorziening	Vraag nieuwe SSL/TLS certificaten aan	Connectie verbetering	BIV32	18.1	Zwakheden in SSL/TLS certificaten	We raden aan nieuwe TLS certificaten aan te vragen waarin de volgende problemen zijn verholpen: De certificaten moeten verstrekt worden door een vertrouwde derde partij die door alle grote browsers ook wordt vertrouwd. Op het interne netwerk betekent dit dat een interne certificaatautoriteit gebruikt moet worden waarvan het root-certificaat op de endpoints geïnstalleerd wordt; Zorg ervoor dat TLS certificaten in de “certificate chain” gebruik maken van RSA keys van minstens 2048 bits en vernieuw alle certificaten die zijn gesigned door de oude certificaten. Zie ook https://www.ssllabs.com/projects/best-practices/index.html voor een gedetailleerde aanpak om SSL op een veilige manier te configureren.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	L	M	L	M	L	Observaties interne infrastructuur test	31-12-2021	Uitgevoerd	KJ	KJ Biometrievoorziening	**26-7-2022:** Onderstaande tickets zijn gesloten en uitgevoerd. Al het verkeer is TLS1.2 TLS1.3 is pas beschikbaar vanaf RHEL8. Wordt op zijn vroegst Q4 2022. **16-07-2021** Nog op te lossen door Biomen-team 5.1.2.i ??? 01-06-2021: Aanvraagproces: 5.1.2.i Contactpersoon: 5.1.2.e @politie.nl
921	Biometrievoorziening	Verbeter het update proces	Implementeer of verbeter het patch/upgrade proces of voer de acties rondom patchen en upgrades door	BIV33	19.1	Verouderde en kwetsbare software geïdentificeerd	We raden aan de systemen te voorzien van de laatste security updates. Verder raden we aan om het update proces aan te scherpen om kwetsbare software tijdig te identificeren. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd.	**Huidige stand van zaken / beantwoording:** De leverancier heeft voor FE inmiddels alle software voorzien van de laatste versie. **Vervolgactie:** Biometrievoorziening zal het patch management beleid en de bijbehorende procedures volgen.	CSC03 Continuous Vulnerability Assessment and Remediation	L	M	L	M	L	Observaties interne infrastructuur test	Gereed	Uitgevoerd	KJ	KJ Biometrievoorziening	**16-07-2021** Leverancier heeft oplossingen opgeleverd, controleren of dit voldoende is. 5.1.2.i
922	Biometrievoorziening	Verwijder overbodige bestanden van webservers	Software matige verbetering	BIV34	20.1	Versie informatie geïdentificeerd	We raden aan geen technische informatie en gedetailleerde versie informatie te tonen. Om dit te bewerkstelligen moet de achterliggende software ingesteld worden om geen versie informatie te tonen in HTTP response headers, via foutmeldingen of op webpagina’s.	**Huidige stand van zaken / beantwoording:** De leverancier probeert het issue te reproduceren. **Vervolgactie:** Het Biomen-team dient input te geven aan leverancier.	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	M	L	L	L	L	Observaties interne infrastructuur test	Nader te bepalen	Niet te reproduceren	KJ	KJ Biometrievoorziening	**15-3-2022** Issue is niet meer te reproduceren ondanks diverse pogingen. Daarom is besloten het issue te sluiten. **16-07-2021** Leverancier probeert issue te reproduceren 5.1.2.i
923	Biometrievoorziening	Verwijder overbodige bestanden van webservers	Software matige verbetering	BIV35	21.1	Overbodige bestanden aangetroffen	We raden aan alle overbodige bestanden te verwijderen van de webserver. Daarnaast bevelen we aan om een proces te implementeren dat periodiek de overbodige bestanden van de server verwijdert.	**Huidige stand van zaken / beantwoording:** De leverancier probeert het issue te reproduceren. **Vervolgactie:** Het Biomen-team dient input te geven aan leverancier.	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	M	L	L	L	L	Observaties interne infrastructuur test	Nader te bepalen	Niet te reproduceren	KJ	KJ Biometrievoorziening	**15-3-2022** Issue is niet meer te reproduceren ondanks diverse pogingen. Daarom is besloten het issue te sluiten. **16-07-2021** Leverancier probeert issue te reproduceren 5.1.2.i
924	Biometrievoorziening	Dwing toegangscontrole af op de Havank backendsystemen	Verbeter autorisatie(s)	BIV36	22.1	Ongeautoriseerde toegang tot gevoelige data	We raden aan logische toegangscontrole af te dwingen voor alle toegang tot gevoelige data. In een ideale situatie wordt dit afgedwongen vanuit een centrale component die gebruikt wordt om enerzijds toegangscontrole af te dwingen en anderzijds weer te geven welke data toegankelijk is voor iedere gebruiker.	**Huidige stand van zaken / beantwoording:** De leverancier werkt aan een oplossing. **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	M	H	H	M	H	Observaties fatclient applicatietest Havank	31-12-2021	In uitvoering: Aangeleverde oplossing dient getoetst te worden.	KJ	KJ Biometrievoorziening	**15-3-2022** Leverancier heeft oplossing opgeleverd, maar deze is nog niet specifiek getoetst. **16-07-2021** Leverancier werkt aan een oplossing 5.1.2.i **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
925	Biometrievoorziening	Geef bijlages in Havank moeilijk te raden identifiers	Verbeter autorisatie(s)	BIV37	23.1	Ongeautoriseerde toegang tot gevoelige data	We adviseren bijlages niet oplopend te nummeren, maar in plaats daarvan willekeurig gegenereerde en moeilijk te raden identifiers te geven, zoals GUID’s, waarmee zij kunnen worden opgevraagd door de gebruikersinterface.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	M	H	H	M	M	Observaties fatclient applicatietest Havank	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
926	Biometrievoorziening	Limiteer de bestandstoegang	Verbeter autorisatie(s)	BIV38	24.1	Local file inclusion via API	De MorphoREST API hoeft alleen configuratiebestanden aan te bieden voor de werking van de applicatie. Het downloaden zou alleen uit de map met configuratiebestanden moeten worden toegestaan. Waar mogelijk moet aan bestanden worden gerefereerd met een identifier waarin het absolute pad naar het bestand niet voorkomt. In plaats daarvan, moet indirect gerefereerd worden aan de bestanden (bijvoorbeeld “het 5e bestand dat kan worden gedownload”).	**Huidige stand van zaken / beantwoording:** Open bug op te lossen door leverancier. **Vervolgactie:** Testen / checken oplevering leverancier.	CSC18 Application Software Security	M	H	H	M	H	Observaties fatclient applicatietest Havank	31-12-2021	In uitvoering: Korte termijn	KJ	KJ Biometrievoorziening	**21-3-2022:** Leverancier geeft aan deze opgelost te hebben. Nog te toetsen. **16-07-2021** Open bug op te lossen door leverancier. 5.1.2.i **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie

930	Biometrievoorziening	Dwing het gebruik van sterke wachtwoorden af	Verbeter autorisatie(s)	BIV42	26.1	Zwakheden in wachtwoordbeleid	We raden aan een strikt wachtwoordbeleid in te voeren en deze te standaardiseren over alle systemen en applicaties. In lijn met het wachtwoordbeleid van de Nationale Politie 2020 raden wij onderstaande beveiligingseisen aan ten aanzien van het wachtwoord: Het wachtwoord bestaat uit ofwel minimaal 20 karakters, ofwel 8 karakters + een tweede authenticatiemiddel; Wachtwoorden die op een blacklist staan mogen niet worden gebruikt; Het wachtwoord mag niet de inlognaam (accountnaam), roepnaam en/of achternaam bevatten; Het wachtwoord bevat karakters uit ten minste 3 van de onderstaande 4 categorieën: Hoofdletters (A t/m Z) Kleine letters (a t/m z) Cijfers (0 t/m 9) Leestekens (bijvoorbeeld: -, !, $, #, %)	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC16 Account Monitoring and Control	M	M	M	M	M	Observaties fatclient applicatietest Havank	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
931	Biometrievoorziening	Maak gebruik van 'certificate pinning'	Connectie verbetering	BIV43	27.1	Gebruikerscertificaten worden geaccepteerd	Wijs een exclusieve certificaatautoriteit aan, welke aan de basis moet staan van het havank.biometrie.politie.local domein. Dit kan bijvoorbeeld het POL-TLSCA zijn die nu de certificaten ondertekend. Andere certificaatautoriteiten moeten door de applicatie worden afgewezen, zelfs als deze in de Windows certificaten store zijn aangemerkt als vertrouwd. Om het moeilijker te maken voor aanvallers om de javax-instellingen aan te passen, zou deze niet als parameter moeten worden meegegeven, maar in de applicatie ingebouwd moeten zijn.	**Huidige stand van zaken / beantwoording:** De leverancier heeft een oplossingsrichting aangeboden. **Vervolgactie:** Het Biomen team zal checken of deze oplossing gaat werken.	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	M	M	M	M	M	Observaties fatclient applicatietest Havank	30-9-2021	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**16-07-2021** Huidige stand van zaken / beantwoording: Leverancier heeft oplossingsrichting aangeboden. Not an issue 2 way SSL not confirgured on DNP site.
932	Biometrievoorziening	Pas filtering toe op de invoer	Software matige verbetering	BIV44	28.1	Beperkte inputfiltering	We raden aan filtering toe te passen op alle invoervelden in de applicatie, om te verzekeren dat slechts geldige invoer wordt verwerkt. In het geval dat een invoerveld bijvoorbeeld alleen cijfers mag bevatten zou de filter alle andere typen invoer moeten weigeren zonder deze invoer door te zenden naar de database. In het geval dat speciale karakters toegestaan moeten worden in een invoerveld, zou de applicatie een standaard functie moeten gebruiken om de speciale karakters te "escapen".	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC18 Application Software Security	M	M	M	M	L	Observaties fatclient applicatietest Havank	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	
933	Biometrievoorziening	Verbeter het update proces	Implementeer of verbeter het patch/upgrade proces of voer de acties rondom patchen en upgrades door	BIV45	29.1	Verouderde en kwetsbare software geïdentificeerd	We raden aan de systemen te voorzien van de laatste security updates. Verder raden we aan om het update proces aan te scherpen om kwetsbare software tijdig te identificeren. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd.	**Huidige stand van zaken / beantwoording:** Check of dit nu opgelost is na nieuwe versie FE en vulnerability scan **Vervolgactie:** Biometrievoorziening zal het patch management beleid en de bijbehorende procedures volgen.	CSC03 Continuous Vulnerability Assessment and Remediation	L	M	L	M	L	Observaties fatclient applicatietest Havank	1-4-2022	In uitvoering: Korte termijn	KJ	KJ Biometrievoorziening	**15-3-2022** 4903 is opgelost, 4759 is in progress. **16-07-2021**: Check of met oplossne vulnerabilities van dit allemaal is opgelost: Oplossing pre livegang applicatie.
934	Biometrievoorziening	Toon geen technische details in foutmeldingen	Software matige verbetering	BIV46	30.1	Technische informatie in foutmeldingen	We raden aan foutmeldingen weer te geven zonder technische informatie over de applicatie of over achterliggende software.	**Huidige stand van zaken / beantwoording:** **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	M	L	L	M	L	Observaties fatclient applicatietest Havank	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	
935	Biometrievoorziening	Dwing toegangscontrole af op de Catch backendsystemen	Verbeter autorisatie(s)	BIV47	31.1	Ongeautoriseerde toegang tot gevoelige data	We raden aan logische toegangscontrole af te dwingen voor alle toegang tot gevoelige data. In een ideale situatie wordt dit afgedwongen vanuit een centrale component die gebruikt wordt om enerzijds toegangscontrole af te dwingen en anderzijds weer te geven welke data toegankelijk is voor iedere gebruiker.	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC14 Controlled Access Based on the Need to Know	M	H	H	M	H	Observaties webapplicatie test Catch	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**16-07-2021** Het issue is uitgezet bij de leverancier. **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
936	Biometrievoorziening	Verwijder de RabbitMQ inloggegevens uit het configuratiebestand	Connectie verbetering	BIV48	32.1	Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd	Verwijder de inloggegevens uit het configuratiebestand 'mvi-config.json', of scherm deze af en gebruik een ander configuratiebestand om naar gebruikers te sturen.	**Huidige stand van zaken / beantwoording:** De leverancier heeft issue opgelost. **Vervolgactie:** Het Biomen-team zal checken of issues zijn opgelost.	CSC14 Controlled Access Based on the Need to Know	M	H	H	M	H	Observaties webapplicatie test Catch	Gereed	Uitgevoerd	KJ	KJ Biometrievoorziening	**16-07-2021** Opgelost door de leverancier, nog te testen / checken door het Biomen team.

937	Biometrievoorziening	Gebruik sterke wachtwoorden voor serviceaccounts	Verbeter autorisatie(s)	BIV49	32.2	Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd	Het wachtwoord van het 'mbss' account bestaat slechts uit enkele letters en is daardoor zwak. Volgens het politiebeleid (januari 2020) wordt het wachtwoord van een serviceaccount willekeurig gegenereerd en is deze "minimaal 30 posities lang, alfanumeriek met vreemde tekens". Verander het wachtwoord van het 'mbss' serviceaccount, aangezien deze mogelijk door gebruikers is ingezien.	**Huidige stand van zaken / beantwoording:** De leverancier heeft issue opgelost. **Vervolgactie:** Het Biomen-team zal checken of issues zijn opgelost.	CSC14 Controlled Access Based on the Need to Know	M	H	H	M	M	Observaties webapplicatie test Catch	Gereed	Uitgevoerd	KJ	KJ Biometrievoorziening	**16-07-2021** Opgelost door de leverancier, nog te testen / checken door het Biomen team. **01-04-2021 Sector IB-Beleid:** Verwijzing naar beleid rondom autorisaties: https://intranet.politie.local/algemenedocumenten/1400/directie-informatievoorziening/privacy-psbd.html#Autorisatie
939	Biometrievoorziening	Beveilig de uploadfunctie	Software matige verbetering	BIV51	34.1	Onveilige bestand upload functie	We raden aan de volgende elementen te implementeren voor alle functies voor het uploaden van bestanden in de toepassing: Toepassen van filtering op basis van bestandsextensie op alle uploadfuncties in de gehele toepassing. Alleen extensies van de vooraf bepaalde 'whitelist' mogen worden toegestaan; Het uitvoeren van bestandstype-detectie en het weigeren van bestanden die niet het juiste formaat van een verwacht bestand hebben; Bestanden laten scannen door een antivirus oplossing.	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC18 Application Software Security	L	M	L	M	L	Observaties webapplicatie test Catch	31-12-2021	Uitgevoerd	KJ	KJ Biometrievoorziening	**26-07-2022** Ticket is gesloten bij de leverancier. Dit wordt afgehandeld met de virusscan van de leverancier (zie ticket) **15-03-2022** : Check update bij Nicolo https://jira.ontwikkel.local/browse/BIOMEN-4709 **16-07-2021** Het issue is uitgezet bij de leverancier
940	Biometrievoorziening	Verbeter de HTTP response header configuratie	Connectie verbetering	BIV52	35.1	Onveilige HTTP response header configuratie	We raden aan de HTTP header configuratie te verbeteren door: De HTTP Strict Transport Security header aan te zetten om het gebruik van SSL/TLS af te dwingen in moderne browsers; Een "allow list" te definiëren in het "Content Security Policy" header veld om in moderne browsers te beschermen tegen potentieel gevaarlijk gebruik van scripts en stylesheets; De cache-control headers (cache-control: private, max-age=0, no-cache) en de pragma header (pragma: no-cache) voor oudere browsers aan te zetten; Anti-clickjacking maatregelen te implementeren, zoals de "X-Frame-Options" header.	**Huidige stand van zaken / beantwoording:** De leverancier heeft issue opgelost. **Vervolgactie:** Het Biomen-team zal checken of issues zijn opgelost.	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	L	M	L	L	L	Observaties webapplicatie test Catch	Gereed	Uitgevoerd	KJ	KJ Biometrievoorziening	**16-07-2021** Opgelost door de leverancier, nog te testen / checken door het Biomen team **26-04-2021** https://jira.ontwikkel.local/browse/BIOMEN-4711
941	Biometrievoorziening	Maak gebruik van de 'Secure Flag' parameter	Connectie verbetering	BIV53	36.1	Onveilig gebruik van cookie parameters	We raden aan het gebruik van cookie instellingen te evalueren en de 'Secure Flag' parameter te gebruiken waar mogelijk. De cookie flags kunnen per cookie worden gezet in de programmacode.	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	L	M	L	L	L	Observaties webapplicatie test Catch	Nader te bepalen	In uitvoering: Plan van aanpak	KJ	KJ Biometrievoorziening	**15-3-2022** Moet de leverancier nog oppakken, minor **16-07-2021** De leverancier bekijkt hoe deze aanbeveling op te lossen. **26-04-2021**
942	Biometrievoorziening	Gebruik standaard foutmeldingen	Software matige verbetering	BIV54	37.1	Technische informatie in foutmeldingen	We raden aan om generieke foutmeldingen weer te geven zonder technische informatie over de applicatie of achterliggende software.	**Huidige stand van zaken / beantwoording:** Het issue is uitgezet bij de leverancier. **Vervolgactie:**	CSC05 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	M	L	L	M	L	Observaties webapplicatie test Catch	Nader te bepalen	Niet te reproduceren	KJ	KJ Biometrievoorziening	**15-3-2022** Issue is niet meer te reproduceren ondanks diverse pogingen. Daarom is besloten het issue te sluiten. **16-07-2021** De leverancier bekijkt hoe deze aanbeveling op te lossen. **26-04-2021**

Roadmap biometrie

«waakzaam en dienstbaar»

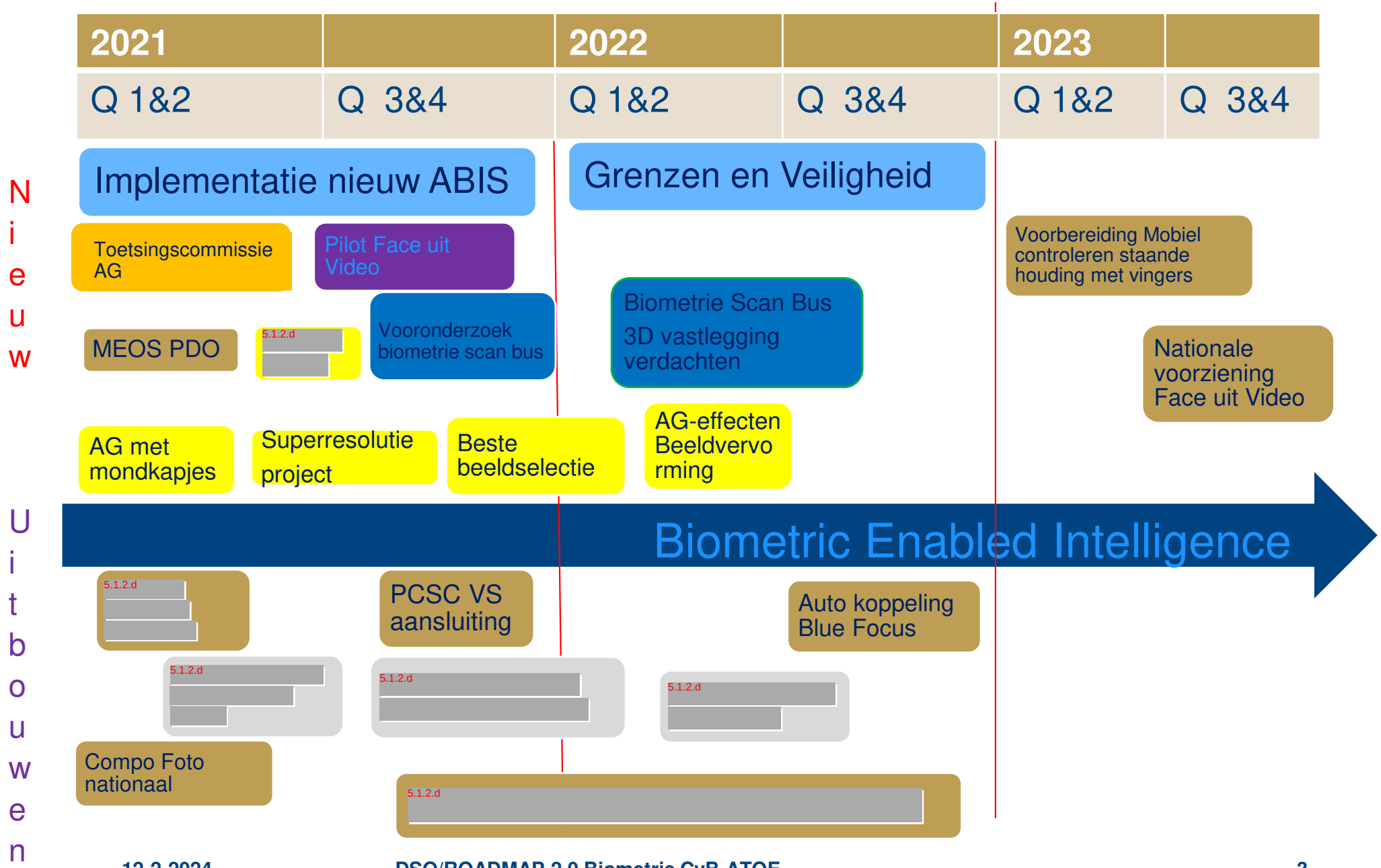
POLITIE

Doel 2024 Roadmap

In 2024 Biometric Enabled Intelligence (BEI) toegevoegd als volwaardig intelligence instrument

BEI is het op basis van biometrie, met kennis, ontsluiten van informatie

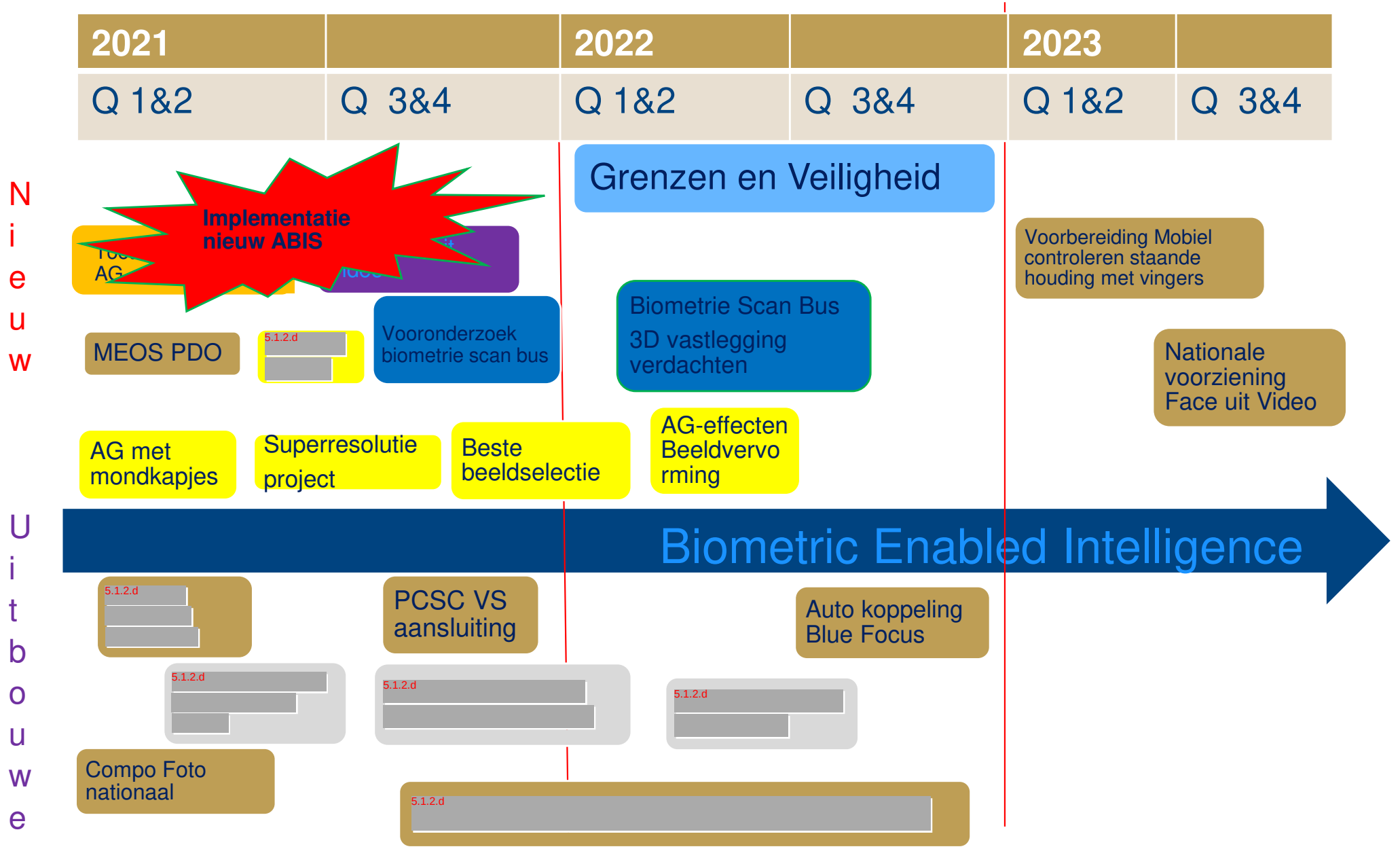
Roadmap in tijd



Legenda Roadmap

- Bruin, projecten zonder onderling verband tussen CvB en ATOE en met andere projecten op de roadmap.
- Lichtblauw, implementatie projecten CvB
- Oranje, gezamenlijke zitting in de toetsingscommissie AG
- Paars, pilot “Face uit video”
- Geel, onderzoekslijn verbetering beelden
- Donkerblauw, Biometrie Scan Bus;3D scanning
- Grijs, 5.1.2.d

Roadmap in tijd



Implementatie van het nieuwe ABIS

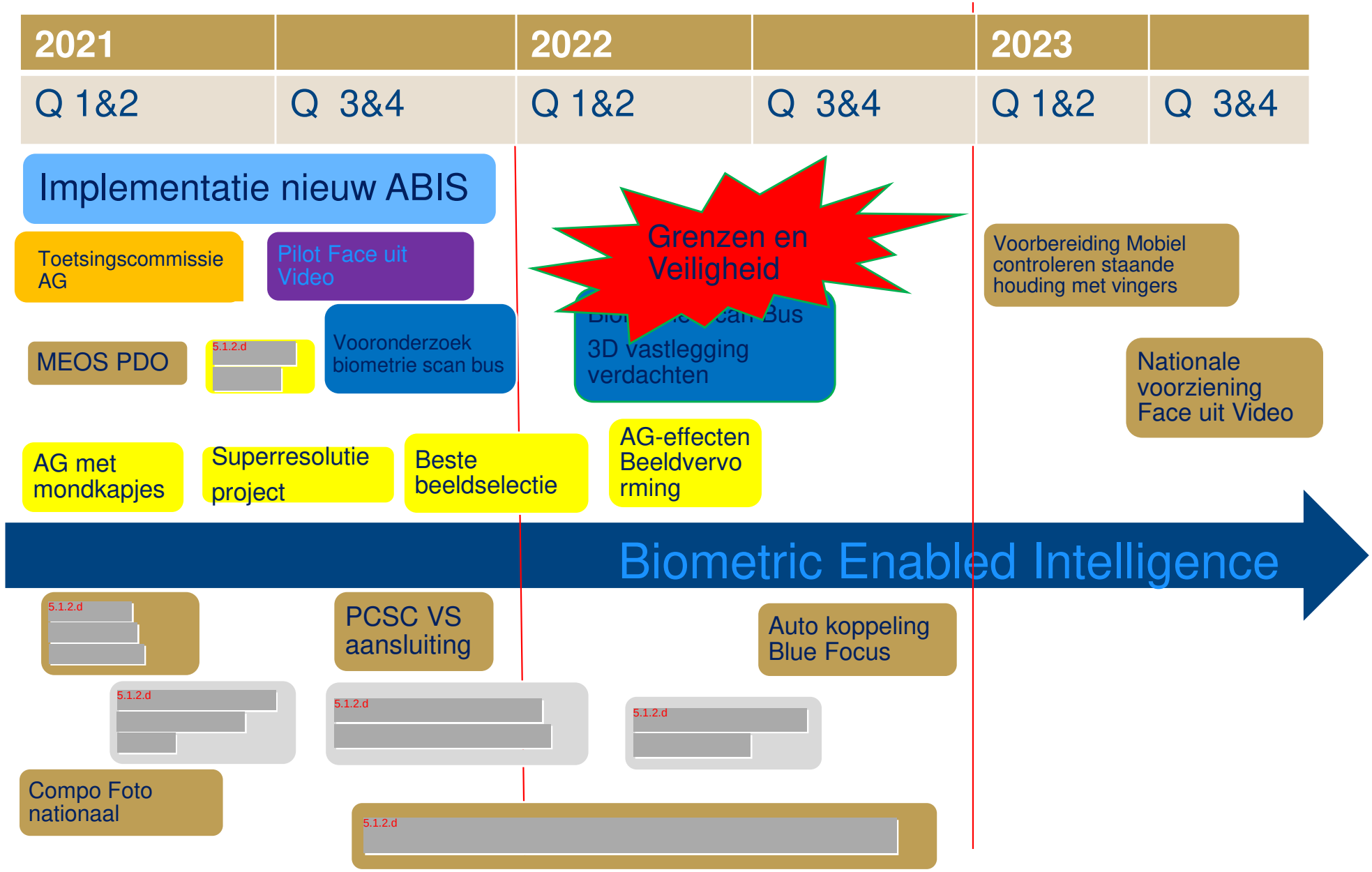
Nieuw verbeterd HAVANK 4 en CATCH 2

Op de Generieke Infrastructuur van de politie

1. Nieuwste algoritmes > hogere terugvindkans
2. Snel uitbreidbaar/opschaalbaar
3. Meerdere database voor verschillende doeleinden
4. Onbeperkt aantal gebruikers
5. API connecties voor ontsluiten naar andere applicaties
6. Basis voor verdere uitbreiding

- HAVANK 4.1.0 operationeel > versie 1.1 en 1.2 komen nog
- CATCH 2.0 wordt oktober/november 2022 verwacht

Roadmap in tijd



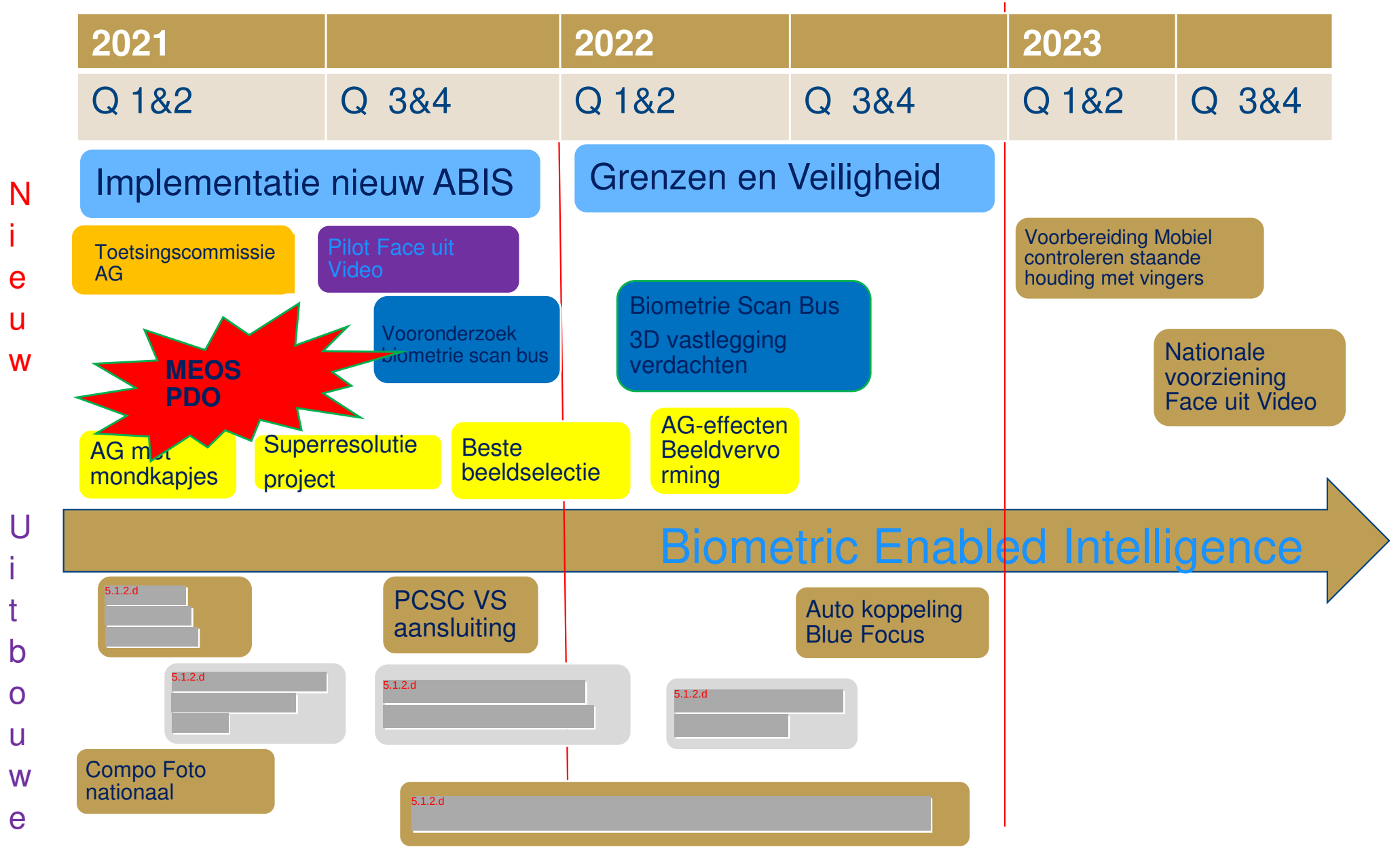
Programma Grenzen en Veiligheid

EU programma voor verbetering toezicht en handhaving EU grenzen

- Biometrie belangrijke rol bij aanvraag, controle en passage EU grenzen
- Bestuursraad J&V heeft besloten dat bestaande expertise centra de Verantwoordelijke Autoriteiten (VA) gaan ondersteunen
- VA's (Kmar, politie, IND, BZ) moeten ook nog worden ingericht
- Aantallen nog onzeker
- Infrastructuur en ondersteunde systemen moeten nog worden beschreven en gebouwd

1 ding zeker > extra werk!

Roadmap in tijd



Plaats Delict Onderzoek app

forensische informatie van ondersteunend naar sturend

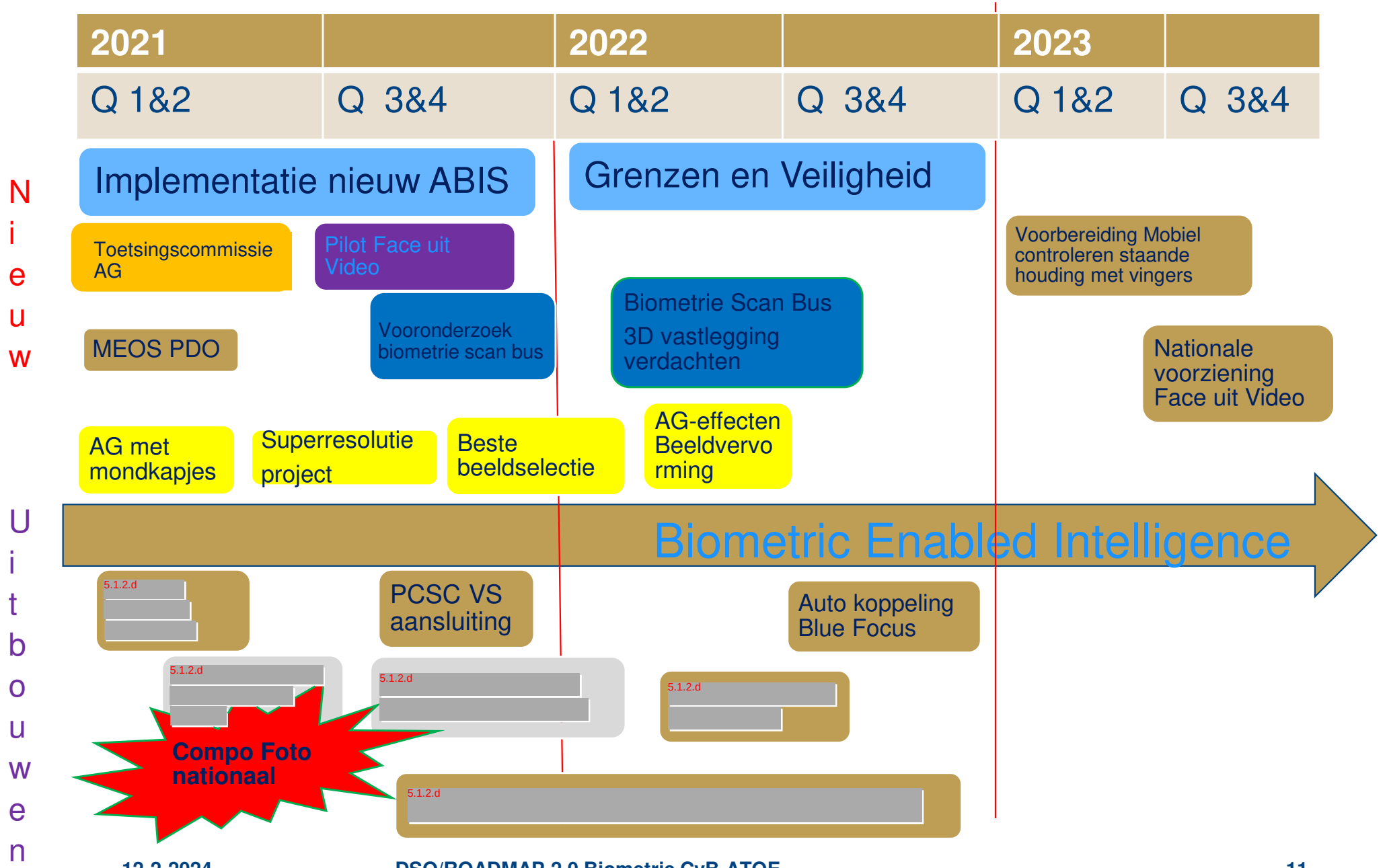
Met een speciale app een foto van dacty spoor vanaf de PD insturen, beoordelen en gelijk zoeken

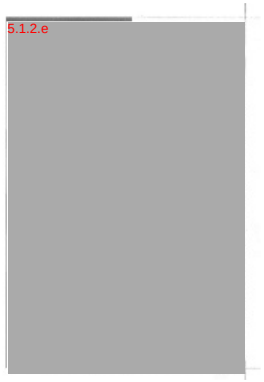
- Zoeken tegen HAVANK met 1,5 miljoen verdachten
- Direct expertise op afstand voor beoordeling kwaliteit spoor terwijl PD open is
- Streven is om binnen 20 minuten (max 3 uur) snel indicatie over identiteit van
  - Slachtoffer
  - Verdachte/Dader
  - Getuigen

- Pre-implementatie proef is afgerond, bevindingen vastgelegd
- HAVANK 4 is PDO gereed
- Aanpassing van de PDO app nog te realiseren > PDO 2.0 staat gepland

****filmpje ****

Roadmap in tijd





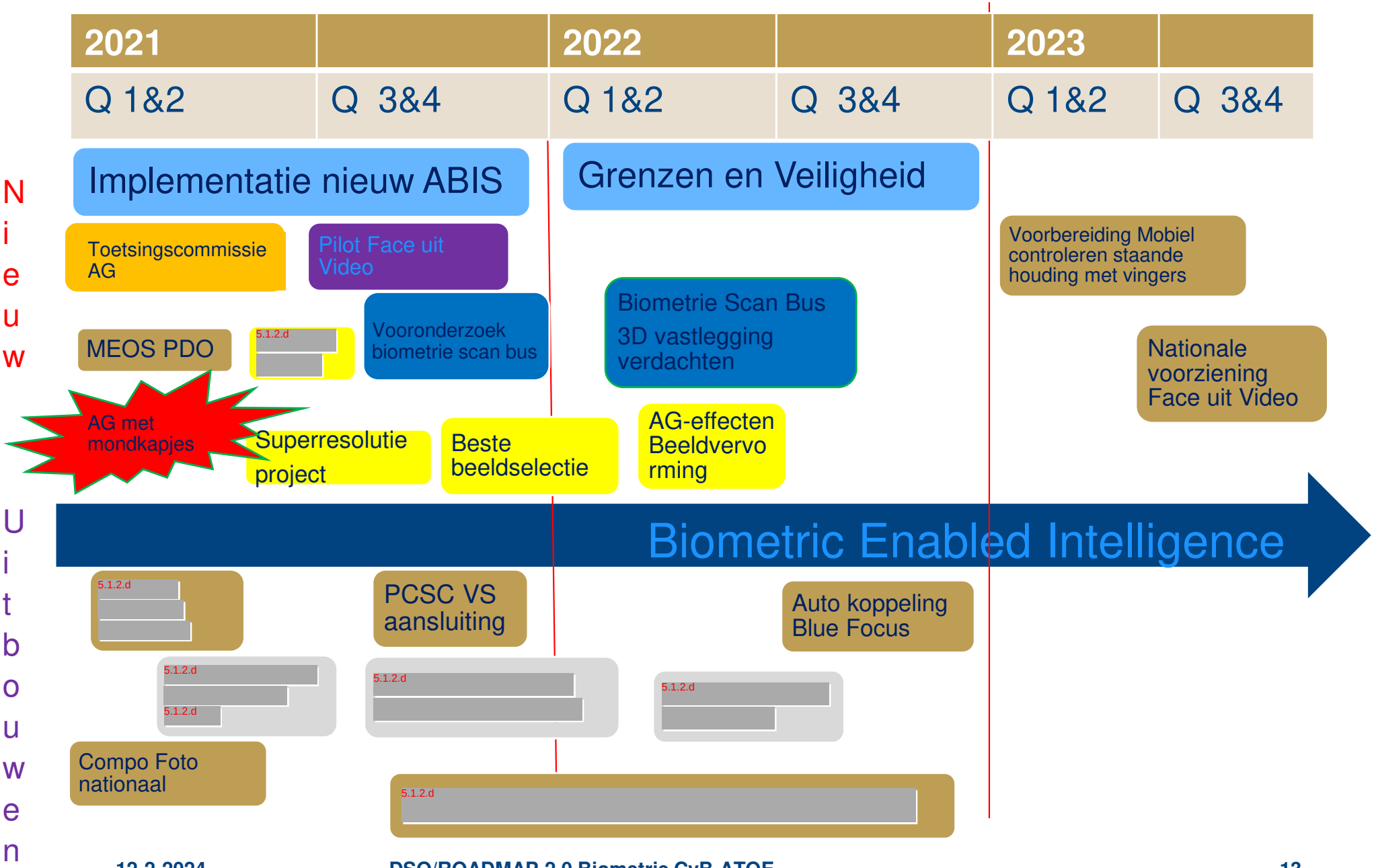
Compo tekenen

Het realiseren van een kwalitatief hoogwaardige productlijn compositietekening en compositiefoto politie breed

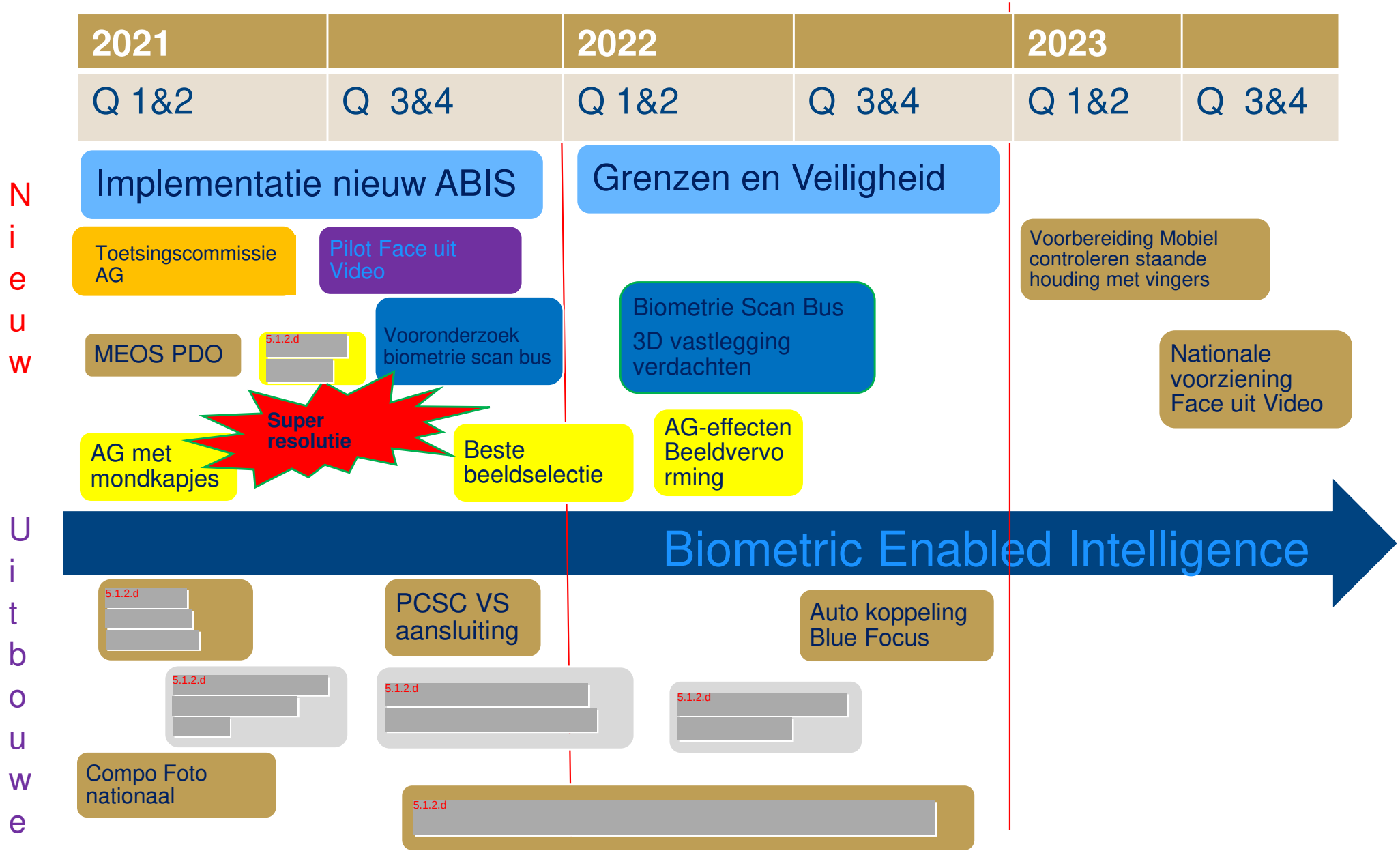
- **Inventariseren huidige situatie**
- **Inrichting politie breed proces**
  - Ingericht proces
  - Systeem ter ondersteuning
  - Competentie eisen tekenaars

- **2 tekenaars in dienst en inzet voor het gehele land**
- **Competentie eisen opgesteld**
- **Ondersteunende systemen in basis beschikbaar**
- **Nog goedkeuren competentie eisen**
- **Opzetten database gezichtskenmerken**

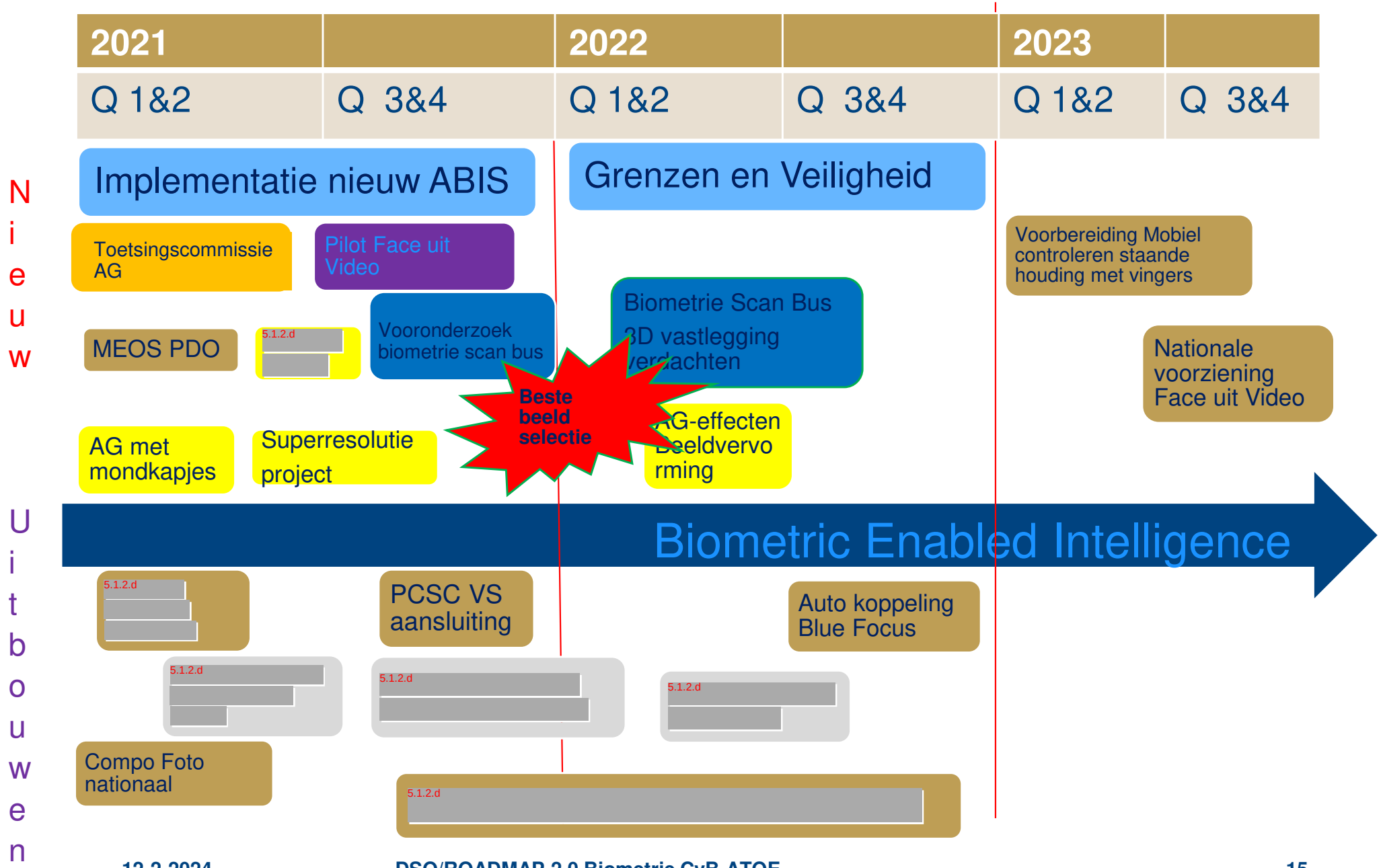
Roadmap in tijd



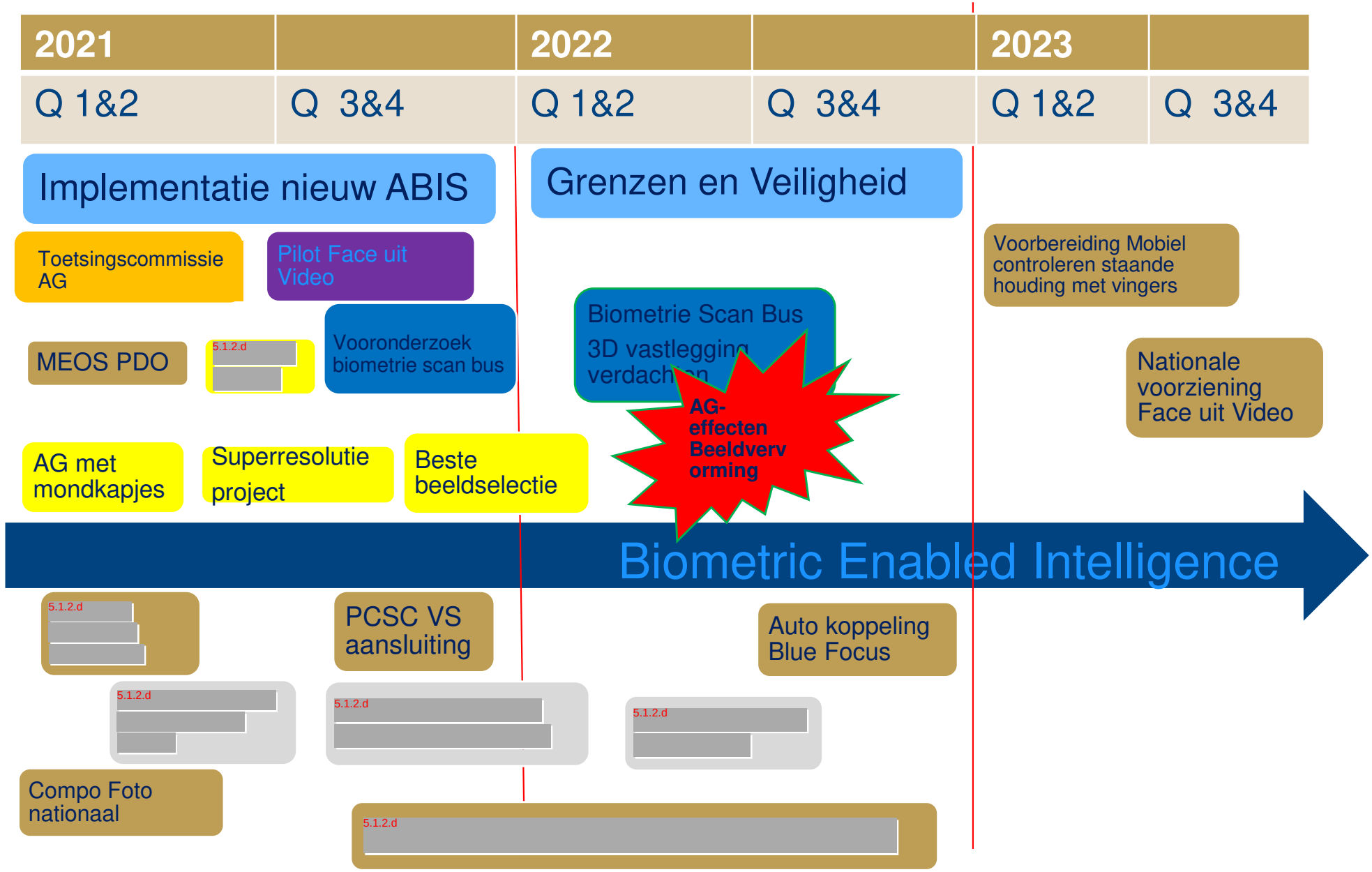
Roadmap in tijd



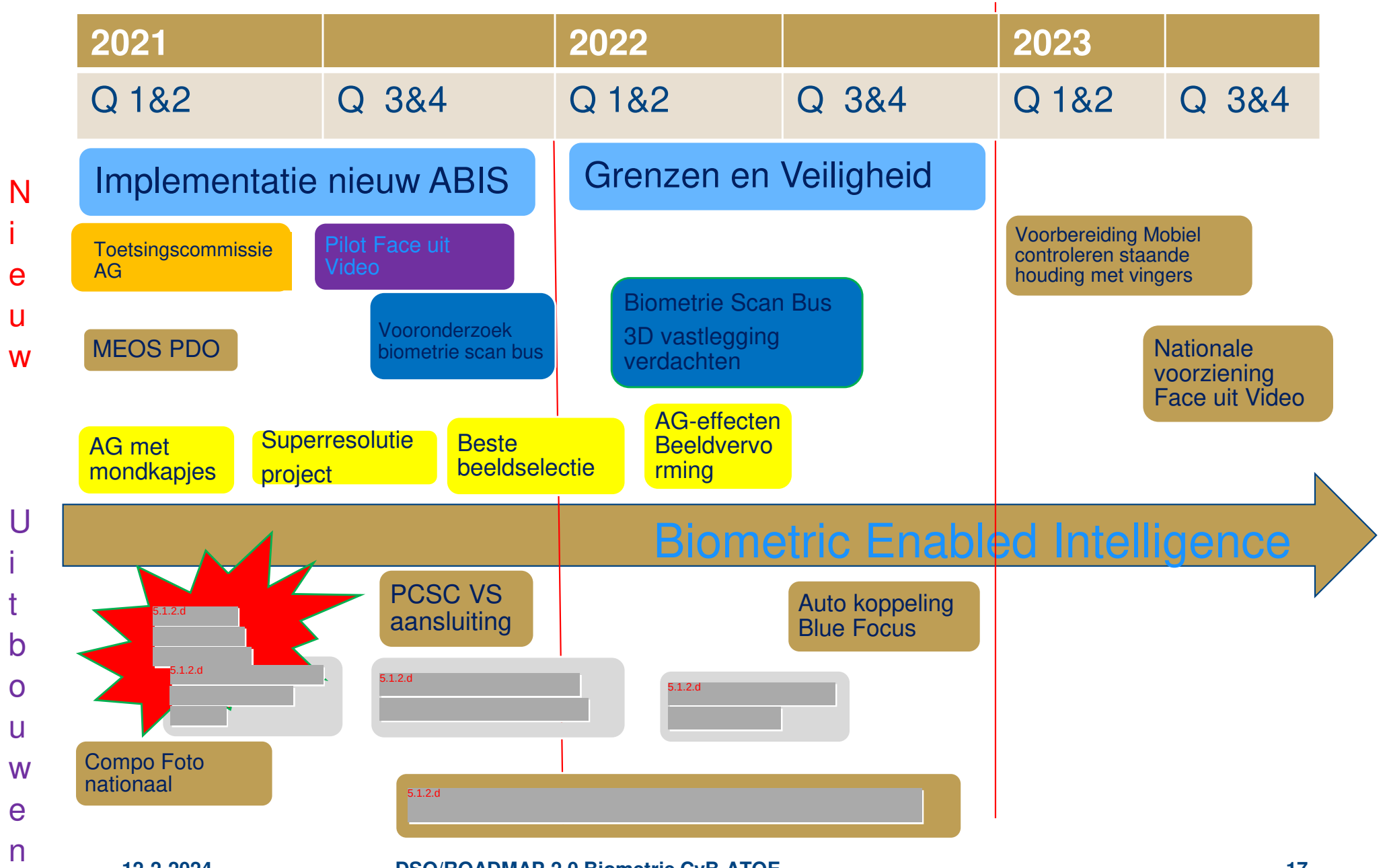
Roadmap in tijd



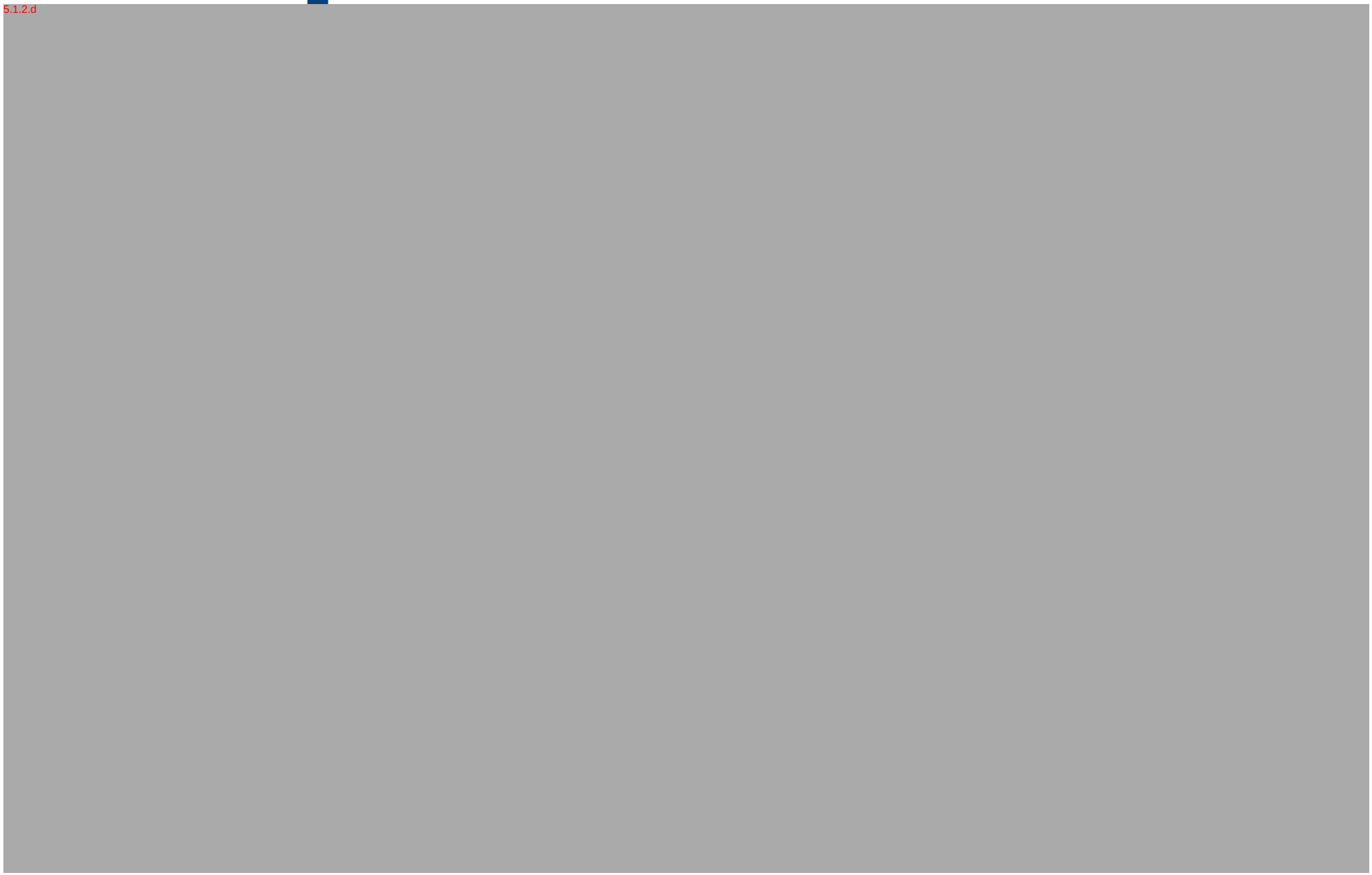
Roadmap in tijd



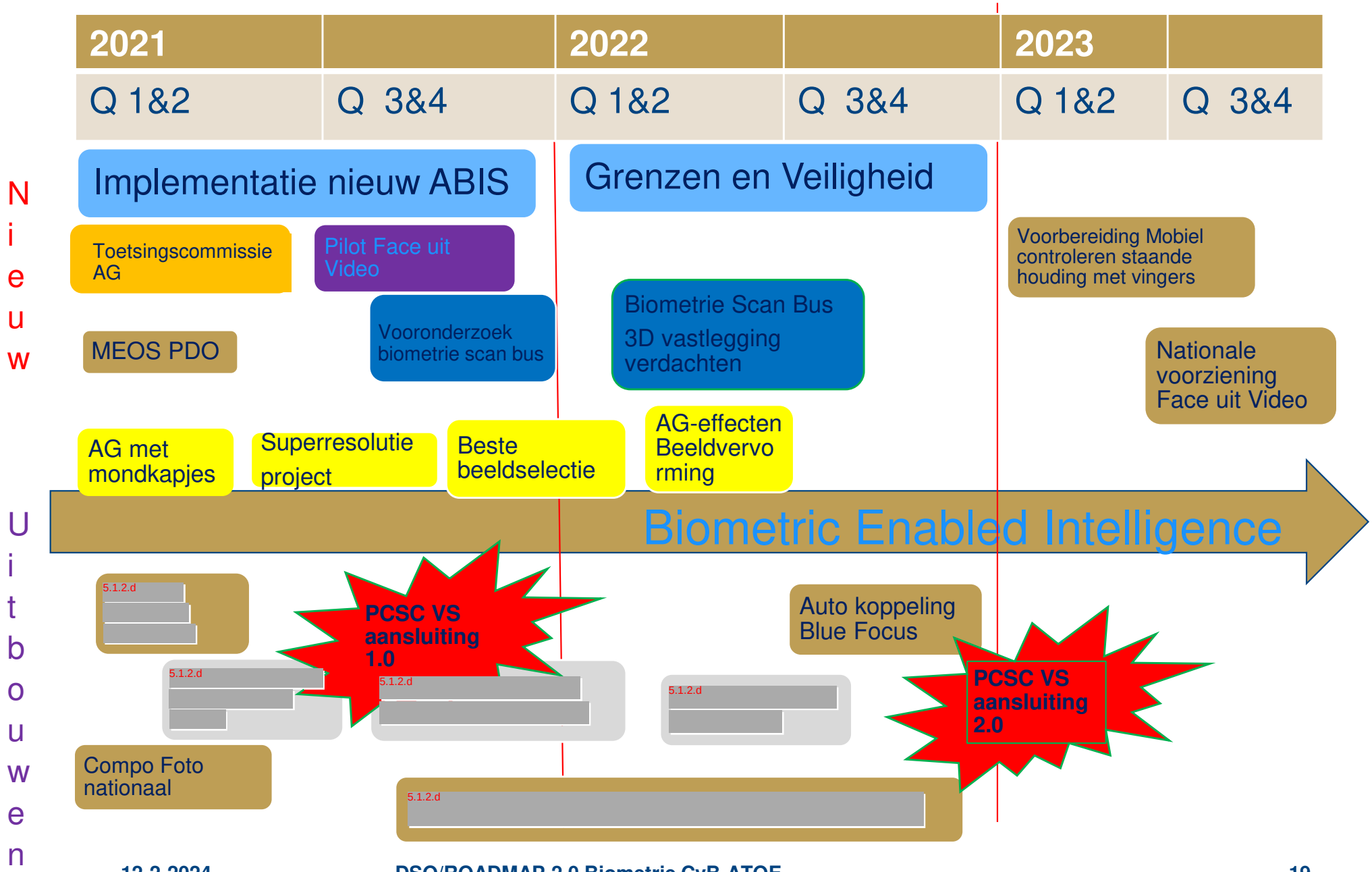
Roadmap in tijd



Opzetten maatwerk onderzoek



Roadmap in tijd



Implementatie PSCS verdrag dacty

- Verdrag voor on-line toegang tot dacty databases van de VS en vice versa

FBI criminele database
70 miljoen verdachten en veroordeelden

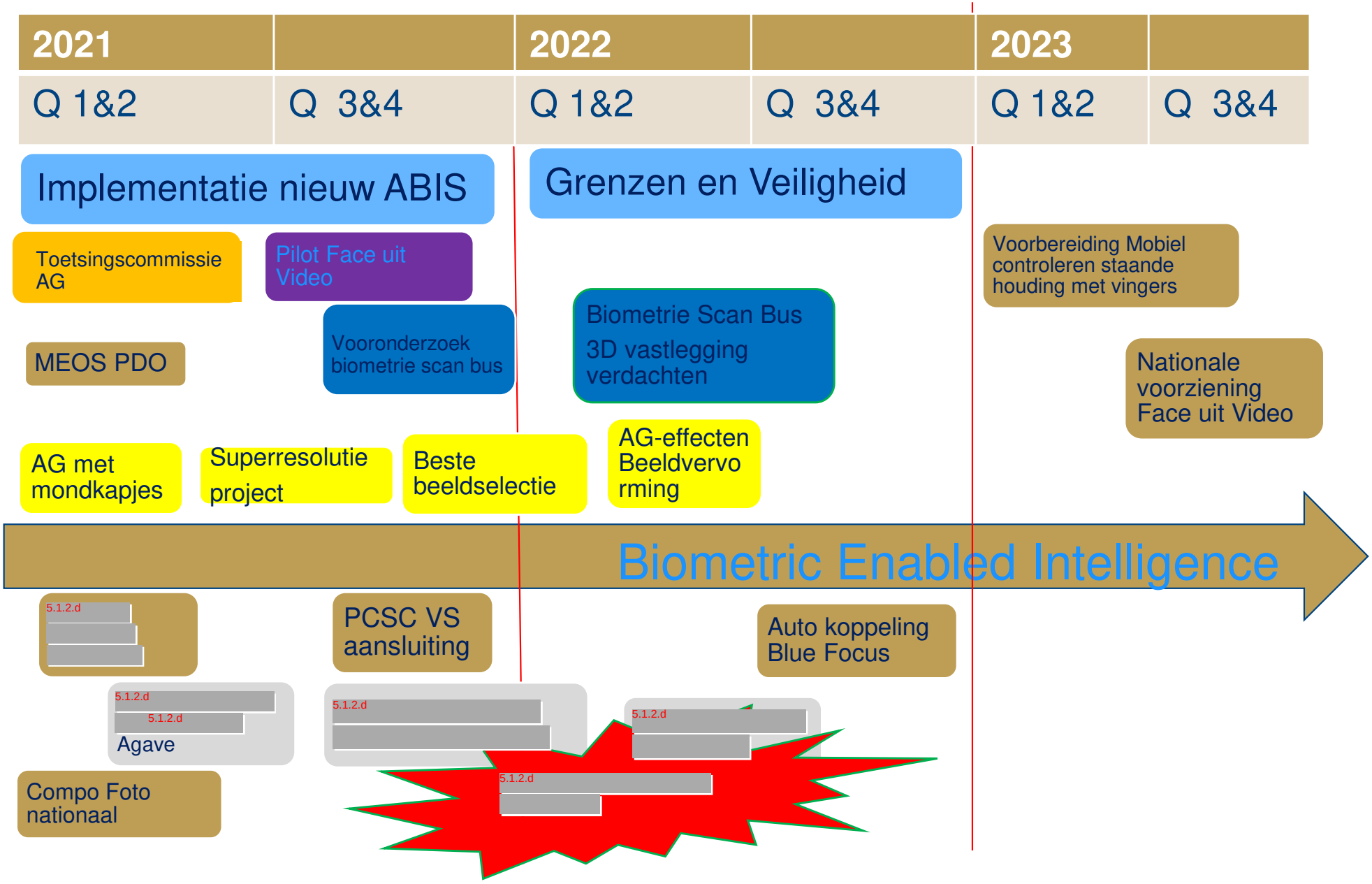
- Personen - Personen
- Sporen - Personen
- Personen – Sporen
- Sporen - Sporen

Departement of Homeland Security, visa
140 miljoen reizigers

- Personen - Personen
- Sporen - Personen

- Handmatige oplossing 1.0 geïmplementeerd en operationeel
- Project PCSC 2.0 moet volledig geautomatiseerde koppeling opleveren

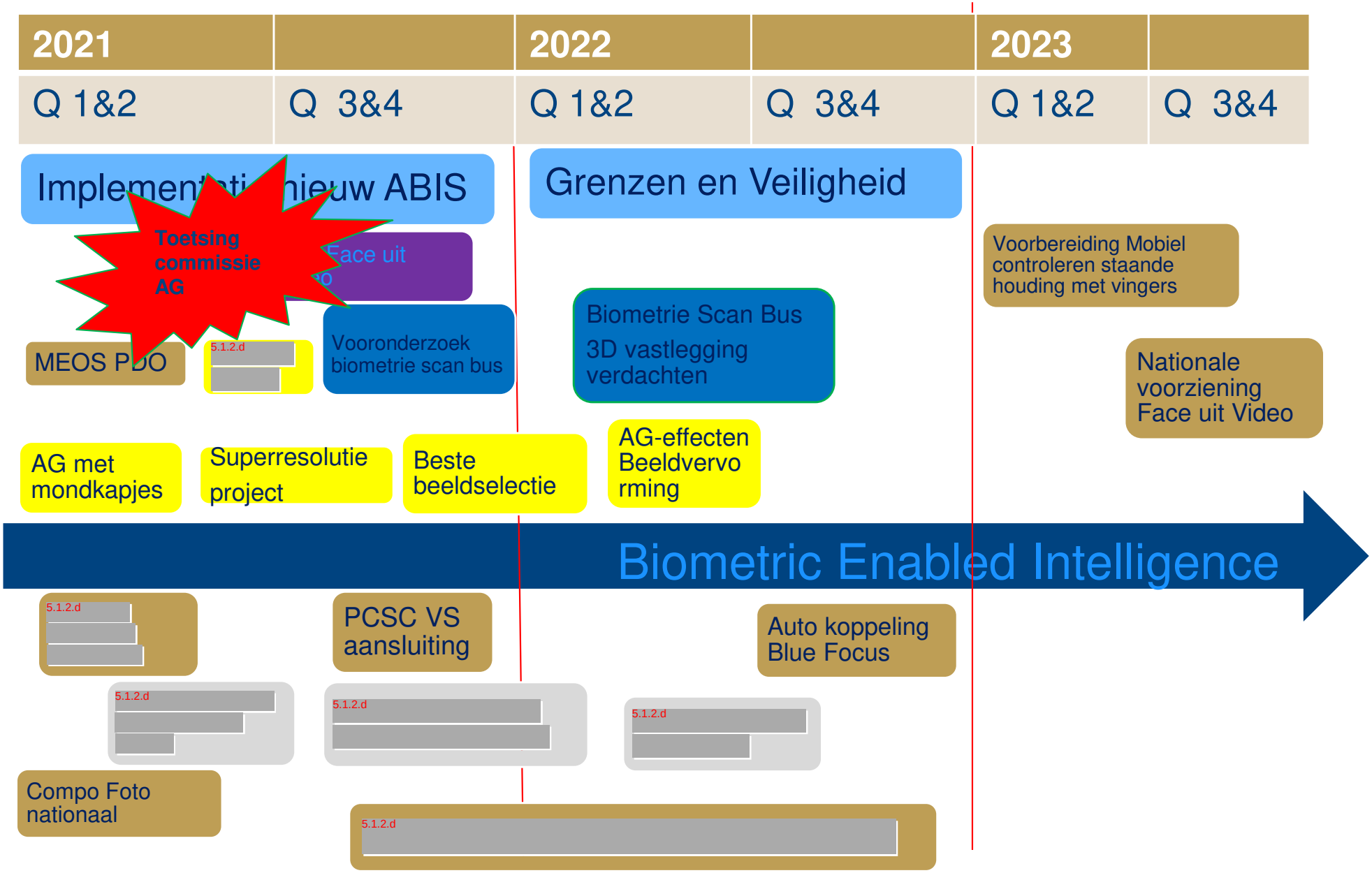
Roadmap in tijd



Specifieke databases

5.1.2.d

Roadmap in tijd



Toetsingscommissie AG

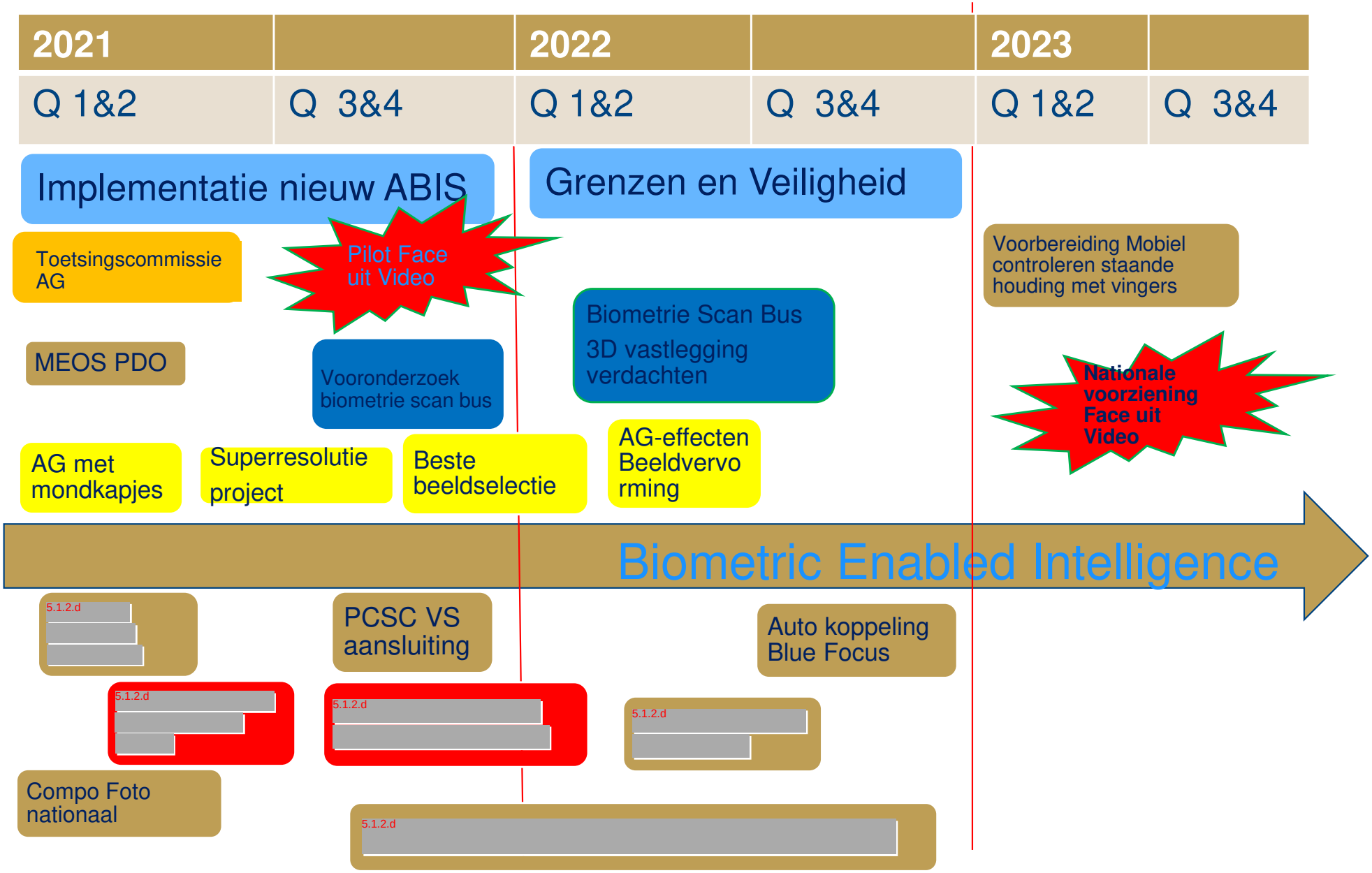
In opdracht van de Minister van J&V opzetten van toetsingskader inzet Automatische Gezichtsherkenning

- **Kernleden hebben het NL kader opgezet**
  - Juridisch
  - Ethisch
  - Technisch

- **Actieve deelname aan een internationaal kader (policy paper) ism UN, WEF en Interpol**
  - Input vanuit praktijk en meeschrijven
  - Deelname aan kernwerkgroep en workshop sessies
  - Opzet en toetsing selff-assessment
  - Deelname aan conferentie

- **NL kader is in concept klaar en is voorgelegd voor goedkeuring KMT**
- **Toetsingscommissie moet worden ingericht**

Roadmap in tijd



Automatische Video Analyse

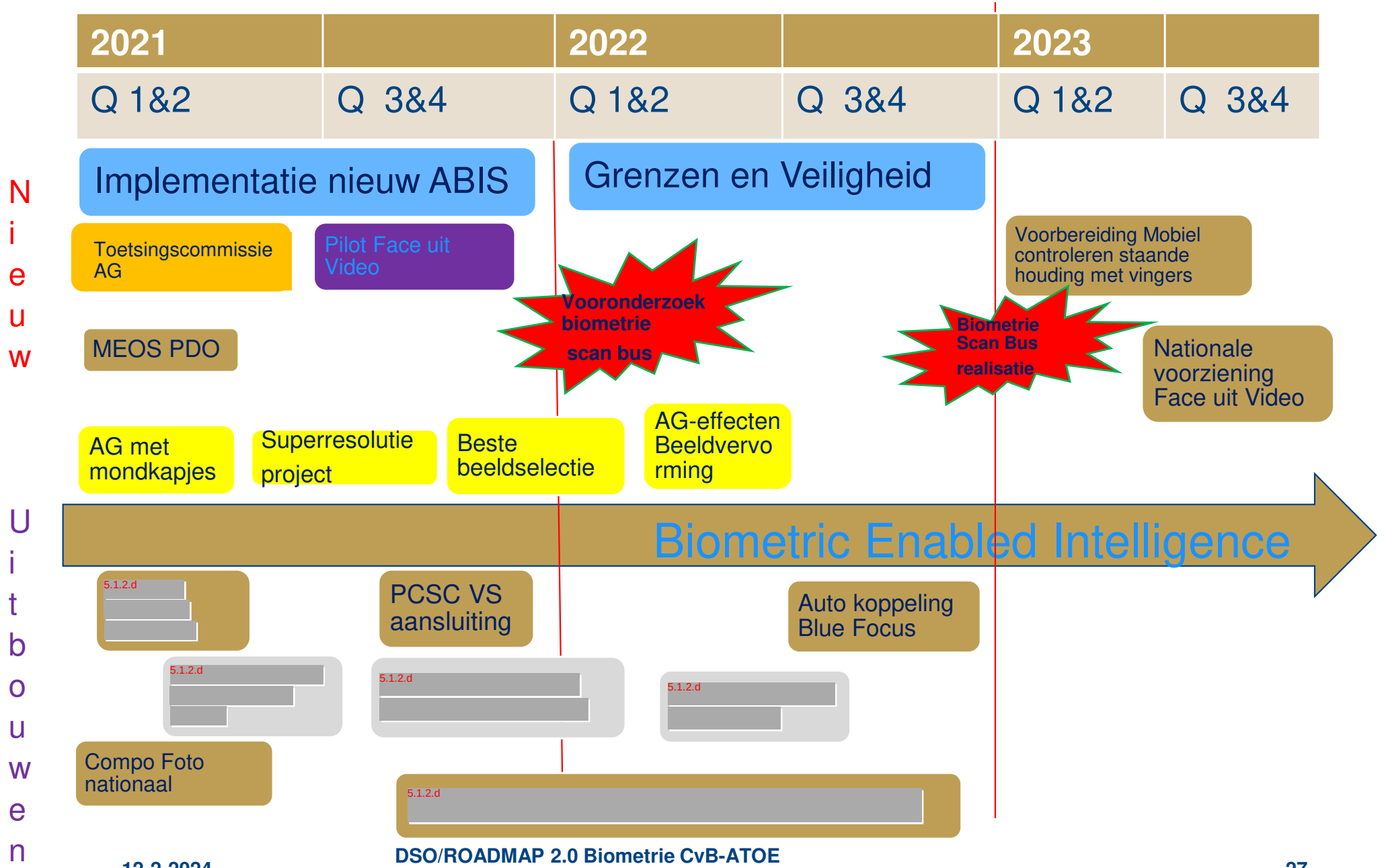
voor gelaatsvergelijking

Automatisch Video Analyseren van bestaande video:

- Detectie waar beweging is
- Detectie waar een persoon in beeld is
- Detectie waar een bruikbaar gezicht in beeld is
- Automatische extractie van herkenbare gezichten
- Zoeken in de database van (herkenbare) gezichten uit de video(s) met signaal waar de gezichten in de video(s) voorkomen
- Zoeken óf 1 of meer personen herkenbaar voorkomen in de video(s)

- IDEMIA product geëvalueerd en input geleverd voor wensen
- Versie 2.0 is gebouwd door IDEMIA en wordt verder geëvalueerd
- Afspraken met TROI Amsterdam voor samenwerking
- Vaststellen hoe zich dit verhoudt tot andere projecten DSO Anyvison/Milestone
- AGAVE is door ATOE ontwikkeld maar zal nog wel langs de toetsing moeten, vraag is ook of er behoefte aan is of dat men inmiddels andere producten heeft. Toesting daarvan is een aandachtspunt.

Roadmap in tijd



Mobiele scan faciliteit

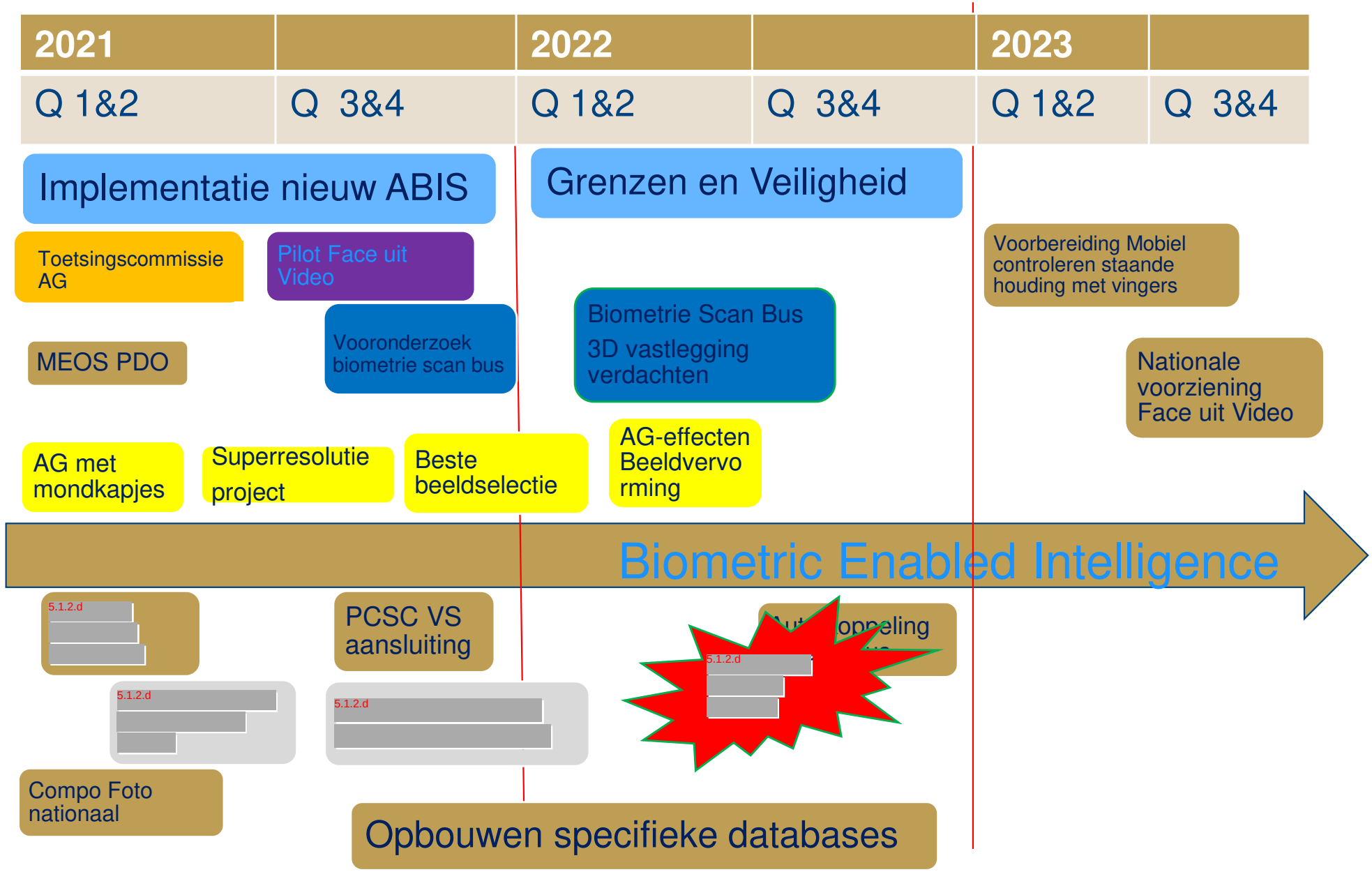
Volledig vastleggen van specifieke verdachten met optimale data voor verbeterde identificatie/herkenning;

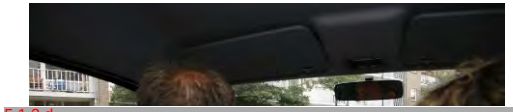
- 3 D persoon inclusief exacte maten
- 2D & 3D gezicht
- Maximale vingerafdrukken (plat, gerold, toppen)
- Volledige handpalmen
- (Blote)voetafdrukken
- Iris
- Tattoo
- etc

Use case CTER subjecten die mogelijk aanslag zullen plegen

- Vooronderzoek afgerond
- Realisatie bus afhankelijk van levering bus

Roadmap in tijd

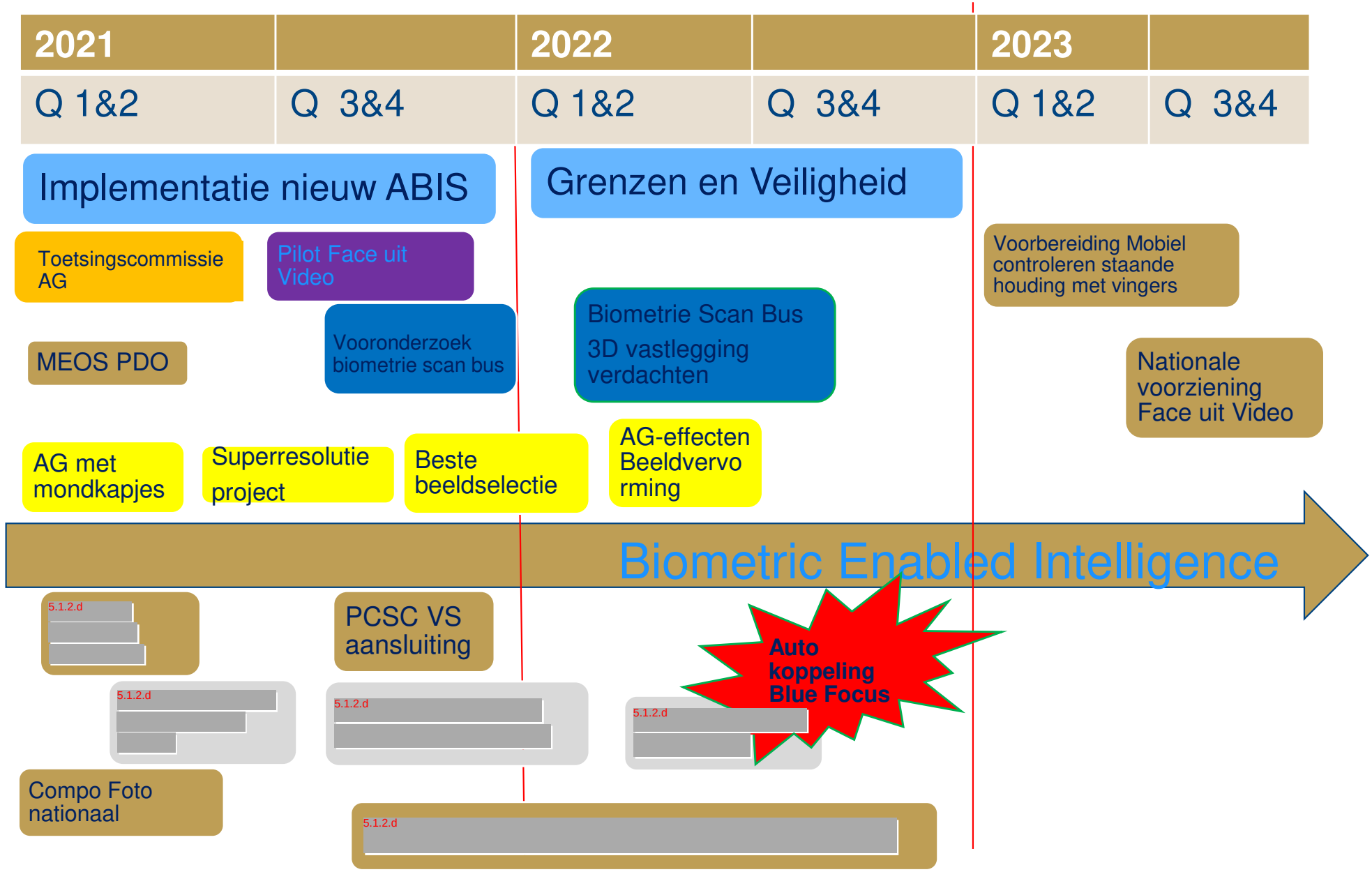




Project AG4OT

5.1.2.d

Roadmap in tijd



Auto Koppeling Blue Focus

Blue Focus “Ter Herkenning” beelden op politie Intranet

Foto’s en stills van video door collega's geplaatst met de vraag om herkenning

5.1.2.e

1. **Bij aanvraag Blue Focus plaatsing automatisch aanbieden of de foto ook in CATCH gezocht moet worden**
2. **Automatisch bepalen of de kwaliteit van de foto voldoende is voor CATCH zoeking**
3. **Blue Focus aanvraag gebruiken als registratie Aanvraag CATCH**

- **Proef met het handmatig downloaden van Blue Focus plaatsingen afgerond**
- **Sponsor voor uren voor maken directe koppeling Blue Focus CATCH 2.0**

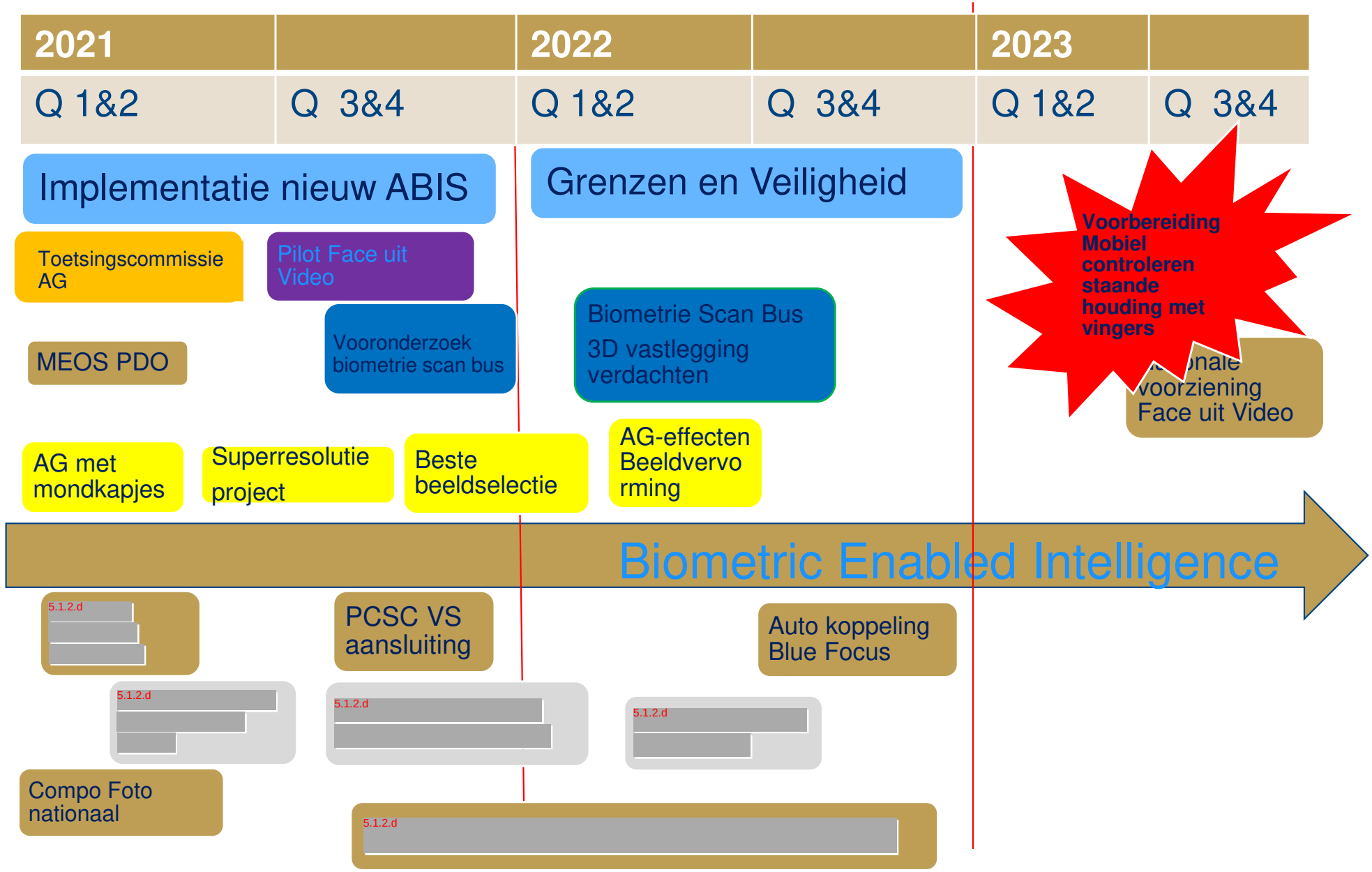
****Zaak AK 47****

- Om 15.15 geplaatst op Blue Focus door de collega's van Rotterdam
- Om 15.21 zelfstandig als spoedverzoek opgepakt door CvB en direct gezocht in CATCH
- Om 16.10 mogelijke herkenning
- OM 17.15 volledig afgehandeld (zoeken + 1 op 1 vergelijking door 2 experts)

en teruggekoppeld dat er een

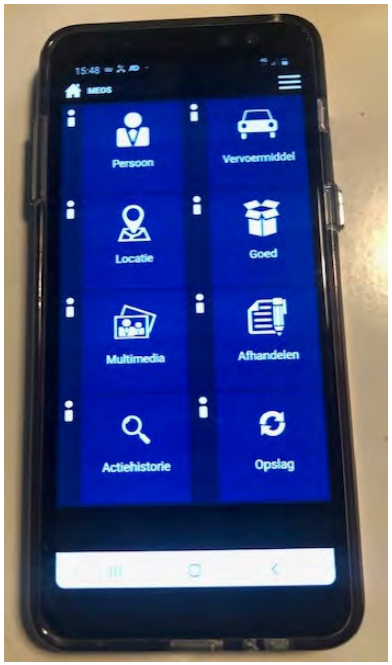
Persoon in de databank is gevonden met CATCH
die veel morphologische overeenkomsten heeft met de persoon op de foto met de AK 47

Roadmap in tijd



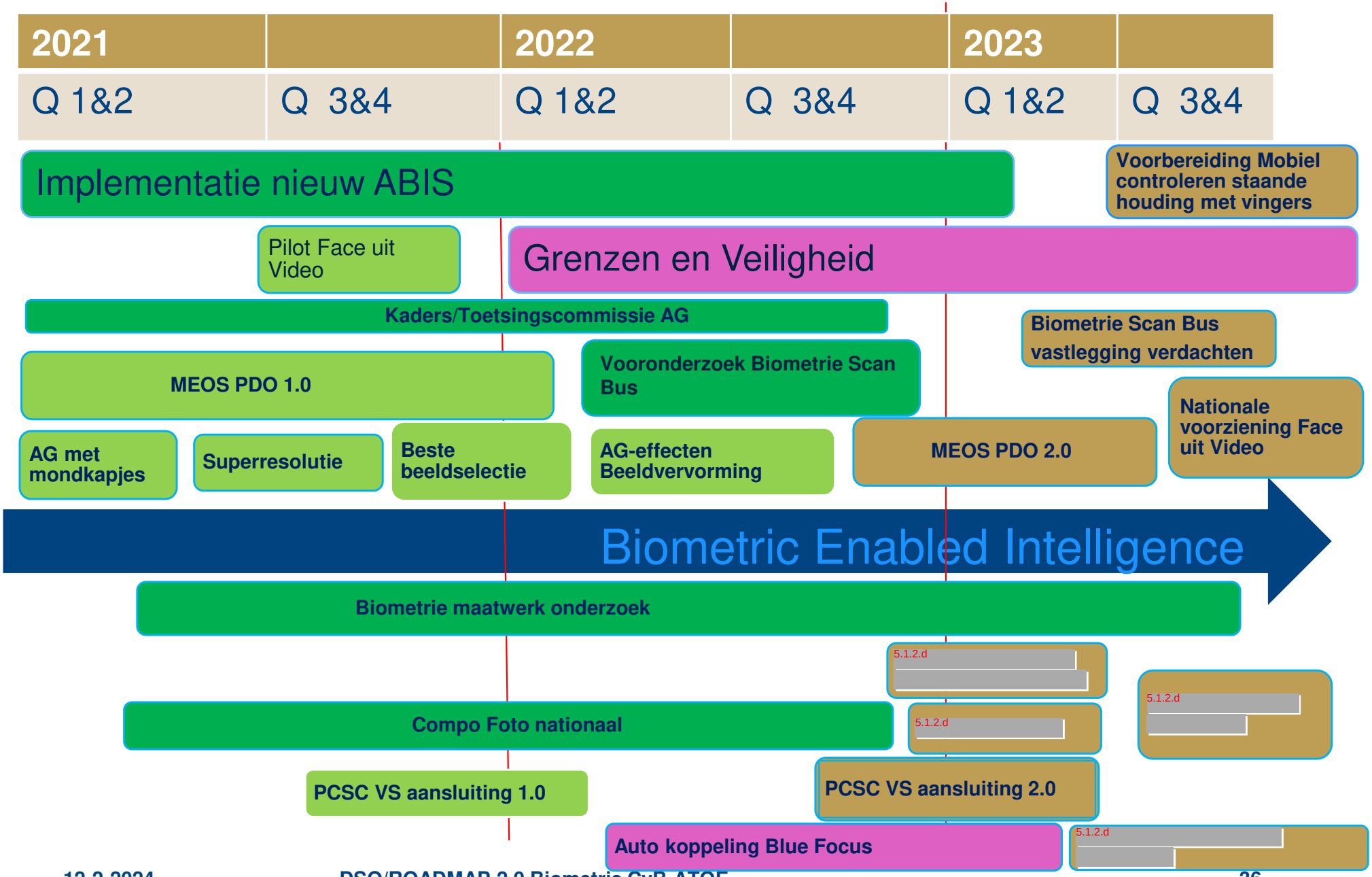
Staande houding en twijfel over ID

- **Wijziging Strafvordering; staande houding en twijfel dan de mogelijkheid om mobiel op straat de vingers te gebruiken voor ID controle**



- Direct fotograferen vingers
- Zoeken tegen algemene én specifieke databases HAVANK

Roadmap in tijd



Legenda Roadmap 2.0

- Lichtgroen, gerealiseerd en afgesloten
- Donkergroen, gerealiseerd maar nog niet volledig klaar
- Roze: start gemaakt maar nog significant werk en keuzes
- Bruin, nog te realiseren

Doel 2024 Roadmap

In 2024 Biometric Enabled Intelligence (BEI) toegevoegd als volwaardig intelligence instrument

BEI is het op basis van biometrie, met kennis, ontsluiten van informatie