Analysis of alternative verification methods

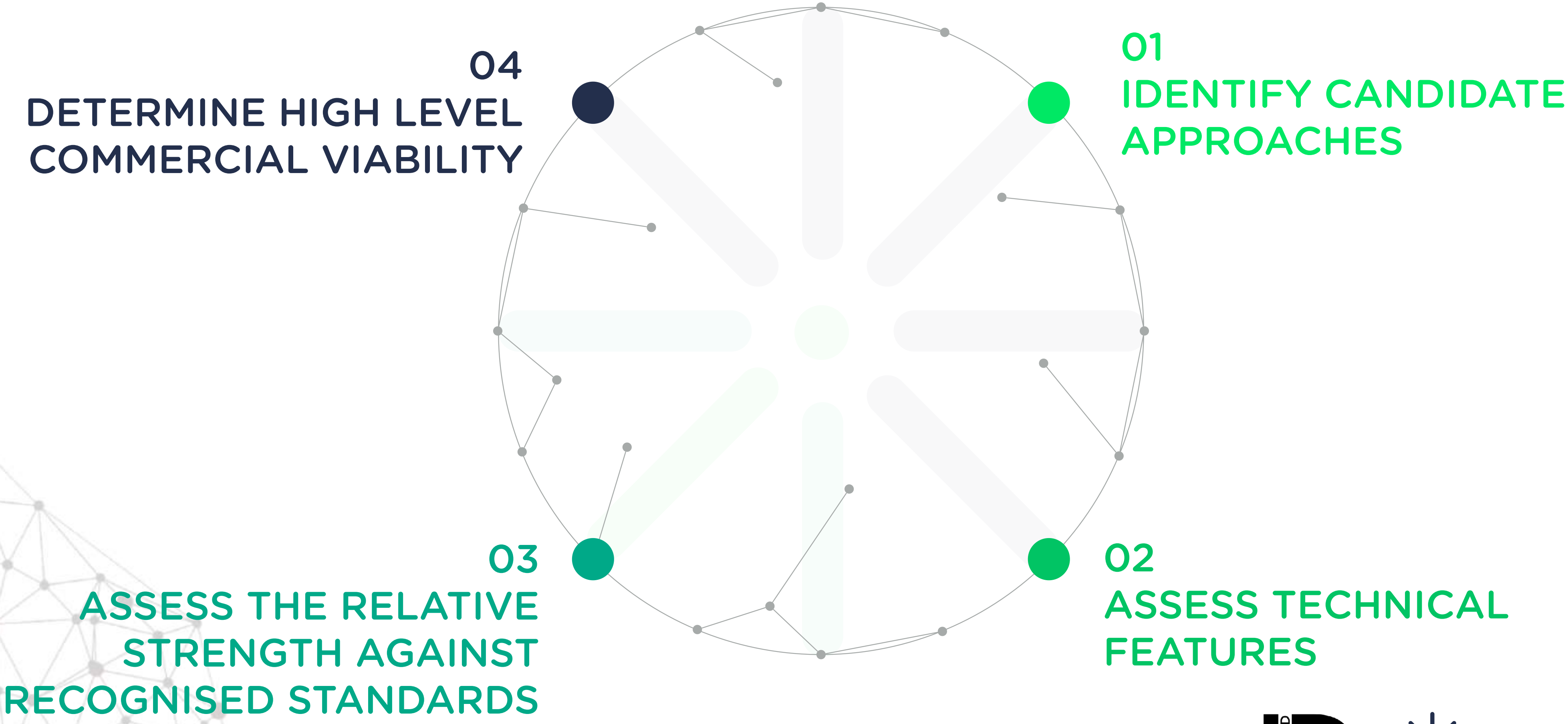
OBJECTIVE

Analysis of alternative verification methods for DHS & DIACC

Propose five or more **methods of verification** that will **provide proof** that the person asserting the identity is the **rightful owner** of the identity.

METHODOLOGY

Analysis of alternative verification methods for DHS & DIACC



01
IDENTIFY CANDIDATE APPROACHES

02
ASSESS TECHNICAL FEATURES

03
ASSESS THE RELATIVE STRENGTH AGAINST RECOGNISED STANDARDS

04
DETERMINE HIGH LEVEL COMMERCIAL VIABILITY

CROWD ID DIGIDENTITY

WHAT WE ASSESSED

- ✓ USE CASES
- ✓ INFORMATION FLOWS
- ✓ VALIDATION CHECKS
- ✓ GENUINE CHECKS
- ✓ CRYPTOGRAPHIC CHECKS
- ✓ CONTRA INDICATOR CHECKS

CROWD ID DIGIDENTITY

EVIDENCE FEATURES

Analysis of alternative verification methods for DHS & DIACC

A description of the **evidence properties** including the required features to mitigate specific threats, including unique identifiers, identity attributes, biometric features, cryptographic features and counter fraud features.

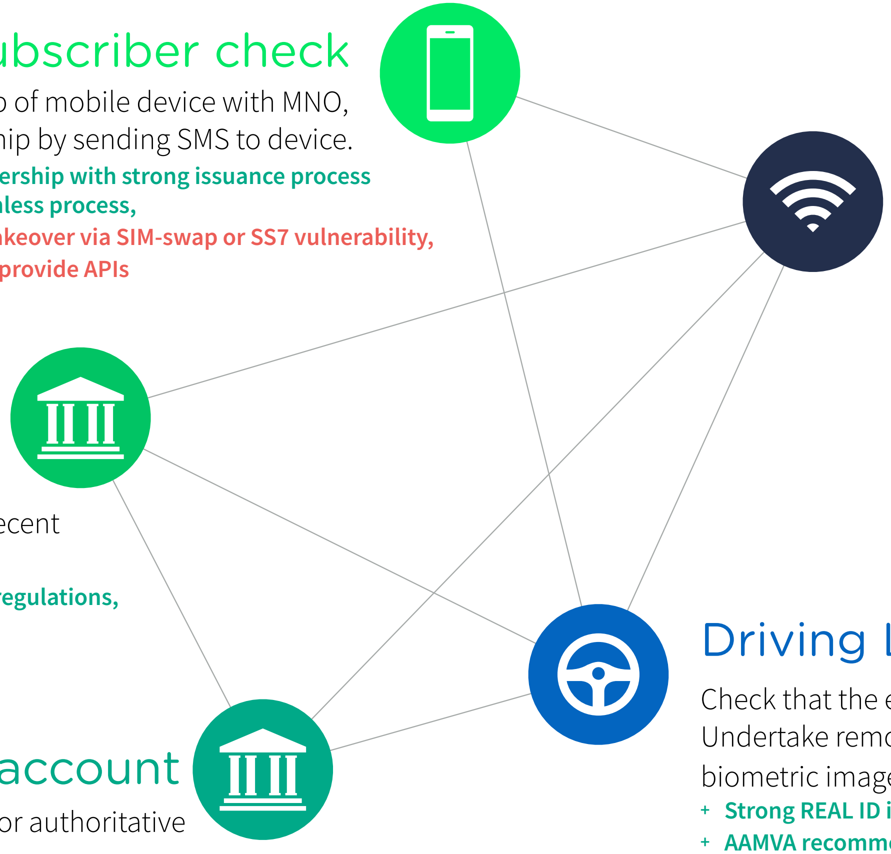
ISSUANCE PROCESS

Analysis of alternative verification methods for DHS & DIACC

- Was an **identity check performed** as part of the issuance process?

- Can it be assumed that the **evidence** was **delivered** into the possession of the individual?

THE FIVE METHODS



Mobile subscriber check

Check ownership of mobile device with MNO,
Confirm ownership by sending SMS to device.

+ High level of ownership with strong issuance process
+ Relatively frictionless process,

- Risk of channel takeover via SIM-swap or SS7 vulnerability,
- Requires MNO to provide APIs

Machine readable travel documents

Check that the evidence is valid and genuine,
Undertake remote comparison between user selfie and biometric image on document.

+ Strong issuance processes,
+ Strong cryptographic features,

- Lack of evidence validation checks against US issuing source
- Low-level of ownership in the US

Financial transactions

Check ownership of financial product with issuing or authoritative source,
Interactive question/answer session based upon recent transactions.

+ Relatively strong issuance process in line with AML/KYC regulations,
+ Highly dynamic dataset,

- Requires financial institutions to provide complex APIs

Verify owner of a financial account

Check ownership of financial product with issuing or authoritative source,
Deposit small amount plus one time passcode into account, user checks A/C & replays OTP to confirm ownership.

+ High degree of online banking usage,
+ Strong issuance process in line with AML/KYC regulations,
+ Utilises existing payments networks,

- Potential time lag due to payment network, high risk of user drop out

Driving Licenses

Check that the evidence is valid and genuine,
Undertake remote comparison between user selfie and biometric image on document.

+ Strong REAL ID issuance processes,
+ AAMVA recommended security features,
+ High Level of ownership in the US,

- REAL ID coverage,
- Lack of security templates for genuine checks

DIGIDENTITY

ALIGNMENT TO NIST 800-63A

Analysis of alternative verification methods for DHS & DIACC

- All methods meet the Identity **Evidence Quality** Requirements as fair to superior

- All methods meet the Identity **Verification Methods** as fair to superior

- These methods could be combined in an identity proofing strategy to achieve Identity Assurance Level 2

Homeland Security

Science and Technology

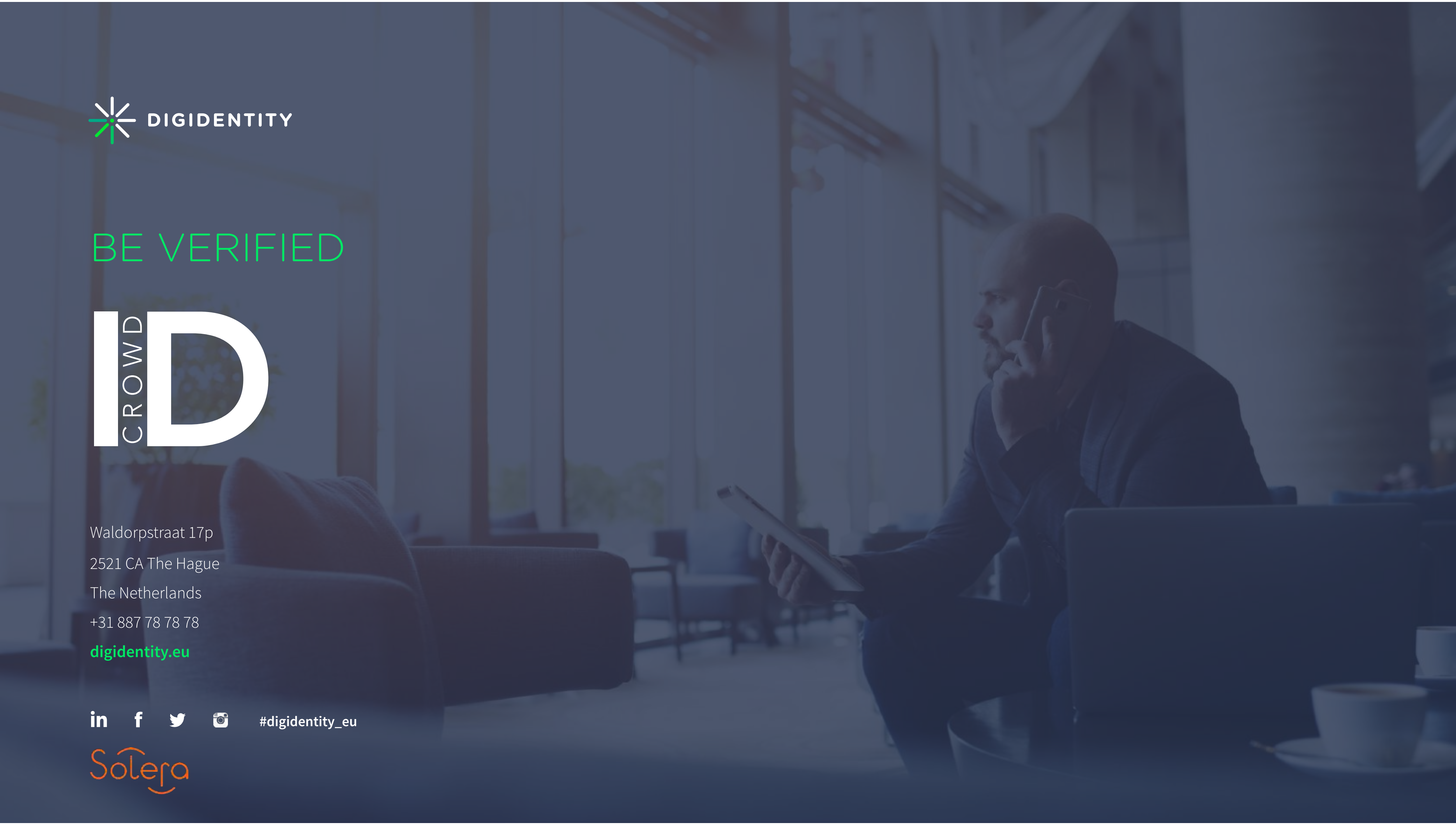
Information in this presentation and/or video is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

For more information, please contact:

Anil John

Program Manager
Cybersecurity R&D

anil.john@hq.dhs.gov



DIGIDENTITY

BE VERIFIED

CROWD ID

Waldorpstraat 17p
2521 CA The Hague
The Netherlands
+31 887 78 78 78
digidentity.eu

#digidentity_eu

Solera