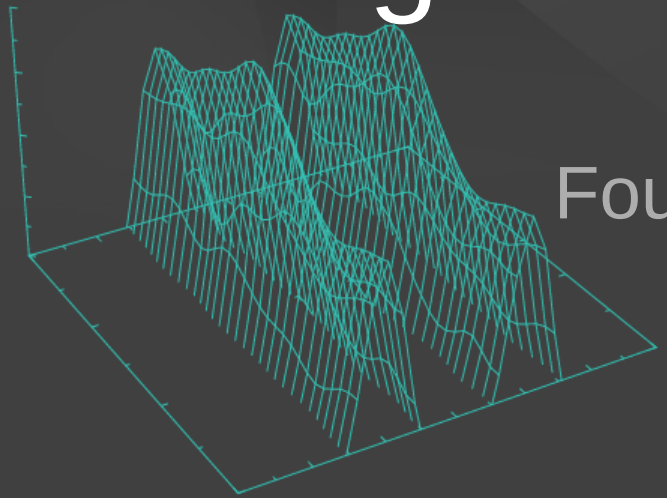
Measuring Authentication: NIST 800-63 Digital Identity Guidelines



Sarah Squire
Founder and Principal Consultant
ENGAGE IDENTITY

@SarahKSquire

Eyewitness News

bartman6: RT @persiankiwi students being killed in tehran uni dorm in amirabad right now. this must stop, ahmadinejad must stop. **#Iranelection**

Jun 14, 2009 11:38 PM GMT · from *web* · Reply · View Tweet

DanValles: RT @persiankiwi: 4am and people still on streets and rooftops shouting 'death to the dictator'. **#Iranelection**

Jun 14, 2009 11:38 PM GMT · from *TweetDeck* · Reply · View Tweet

RodDavis: New proxy server is up for any protesters who need it. IP: 69.92.182.12 Port: 2100 #Iran **#IranElection** #mousavi

Jun 14, 2009 11:38 PM GMT · from *TweetDeck* · Reply · View Tweet

A Play in Four Acts

- ★ What is authentication, and why are we measuring it?
- ★ Levels of Assurance
- ★ NIST Digital Identity Guidelines
- ★ Password and MFA Guidance

What is authentication, and why are we measuring it?

Act I


Burgundy
HUDSONS BAY
SCOTCH WHISKY


Standard size- 750 ml
CHINON
CHINON
DOMAINE
RENÉ COUET
CHINON
LA BARONNIE MADELEINE
CHINON
CHINON
Mathusalem

What is authentication, and why are we measuring it?

What is authentication, and why are we measuring it?

ELI5 version:

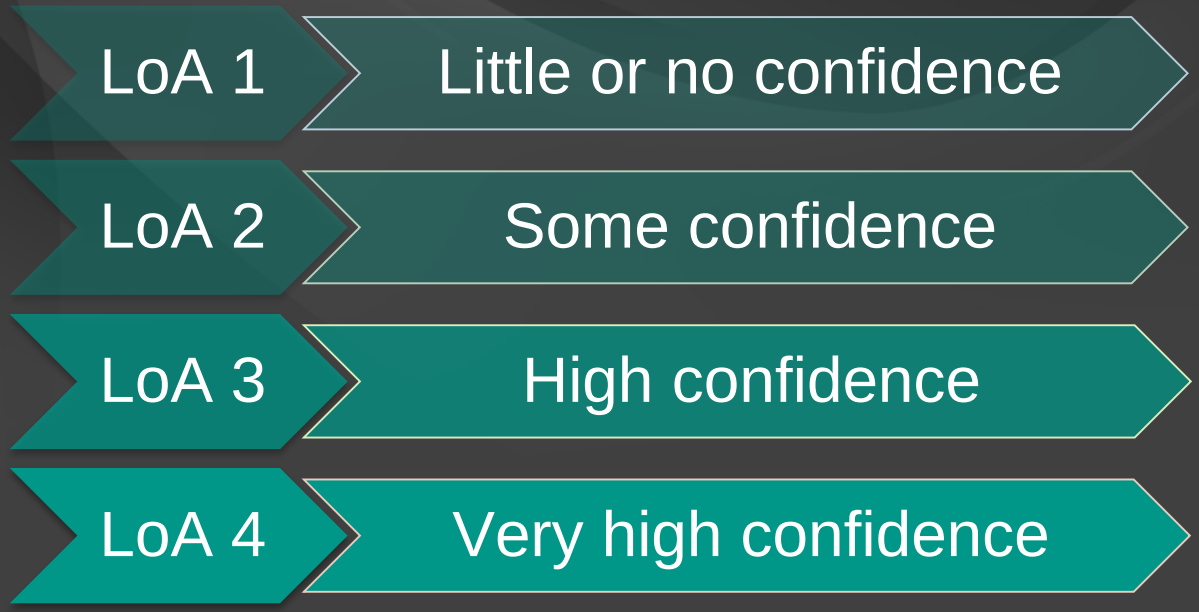
Making sure that a person or thing is the same person or thing you saw last time (which is different from them being who they say they are!)

Levels of Assurance

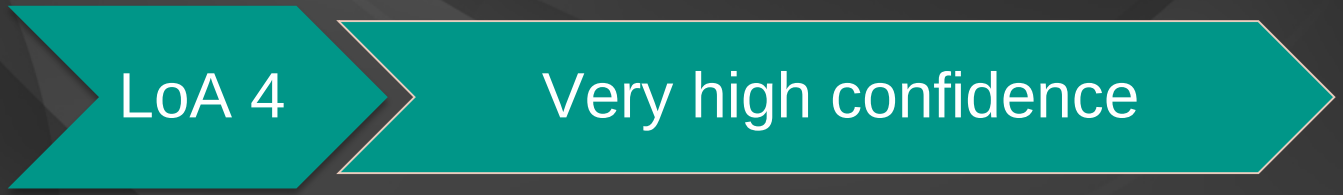
Act II

Levels of Assurance

Levels of Assurance



Levels of Assurance



- Strong cryptographic authentication

Levels of Assurance

LoA 4 — Very high confidence

- Strong cryptographic authentication
- Strong man-in-the-middle resistance

Levels of Assurance

LoA 4 — Very high confidence

- Strong cryptographic authentication
- Strong man-in-the-middle resistance
- No bearer tokens

Levels of Assurance

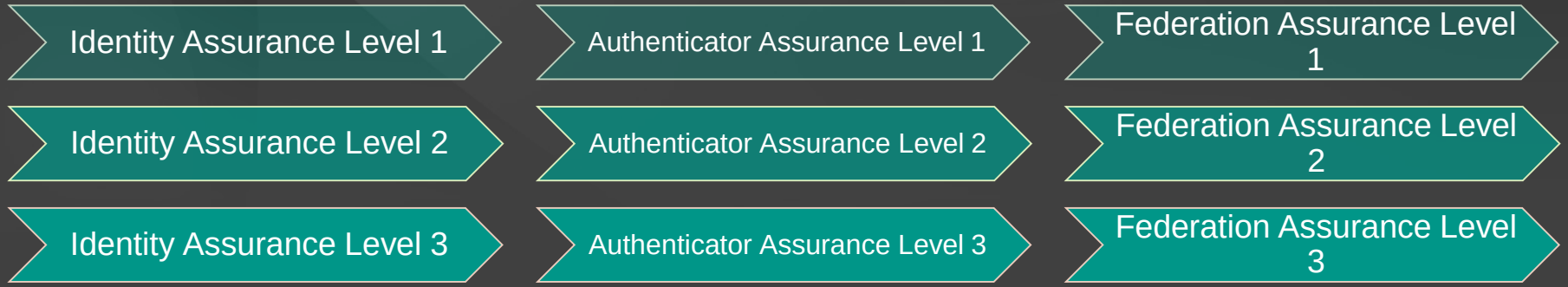
LoA 4 — Very high confidence

- Strong cryptographic authentication
- Strong man-in-the-middle resistance
- No bearer tokens
- Account owner has physically appeared and a government-issued photo-identification document has been verified by the relevant agency.

NIST Digital Identity Guidelines

Act III

NIST Digital Identity Guidelines



Identity Assurance Levels

Identity Assurance Level 1

Pseudonymous

Identity Assurance Levels

Identity Assurance Level 1	Pseudonymous
Identity Assurance Level 2	Remote or In-person identity proofing

Identity Assurance Levels

Identity Assurance Level 1	Pseudonymous
Identity Assurance Level 2	Remote or In-person identity proofing
Identity Assurance Level 3	In-person identity proofing with biometric collection for the purpose of non-repudiation

Authenticator Assurance Levels

Authenticator Assurance Level 1

Single factor authentication

Authenticator Assurance Levels

Authenticator Assurance Level 1	Single factor authentication
Authenticator Assurance Level 2	Two-factor authentication

Authenticator Assurance Levels

Authenticator Assurance Level 1	Single factor authentication
Authenticator Assurance Level 2	Two-factor authentication
Authenticator Assurance Level 3	Two-factor authentication with cryptographic device and verifier impersonation resistance

Federation Assurance Levels

Federation Assurance Level 1

Signed bearer assertion

Federation Assurance Levels

Federation Assurance Level 1	Signed bearer assertion
Federation Assurance Level 2	Signed and encrypted bearer assertion

Federation Assurance Levels

Federation Assurance Level 1	Signed bearer assertion
Federation Assurance Level 2	Signed and encrypted bearer assertion
Federation Assurance Level 3	Signed and encrypted holder-of-key assertion

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level?

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level: 3

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level: 3

Authenticator Assurance Level?

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level: 3

Authenticator Assurance Level: 3

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level: 3

Authenticator Assurance Level: 3

Federation Assurance Level?

NIST Digital Identity Guidelines

Example:
Secretary of State

Identity Assurance Level: 3

Authenticator Assurance Level: 3

Federation Assurance Level: 2

Password and MFA Guidance

Act V

MFA Guidance

Knowledge-based authentication (KBA) is banned

MFA Guidance

Knowledge-based authentication (KBA) is banned

- bad security

MFA Guidance

Knowledge-based authentication (KBA) is banned

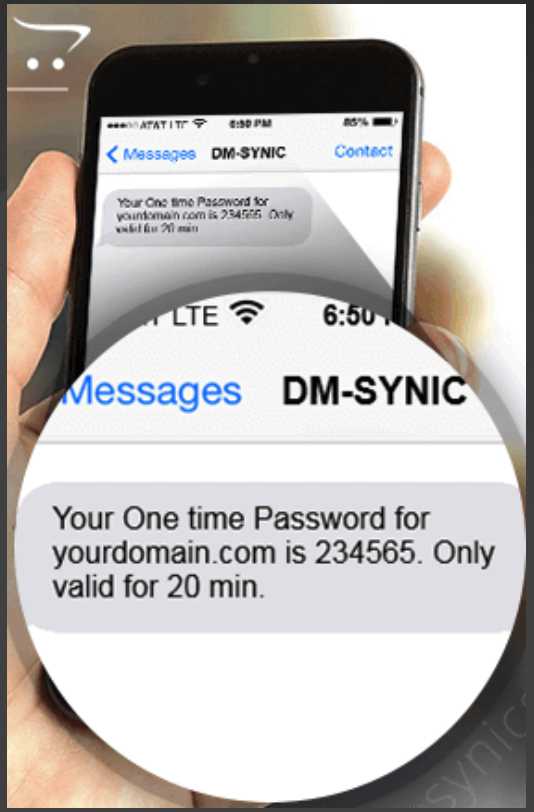
- bad security
- bad usability

MFA Guidance

Knowledge-based authentication (KBA) is banned

- bad security
- bad usability

One-time password over SMS is restricted



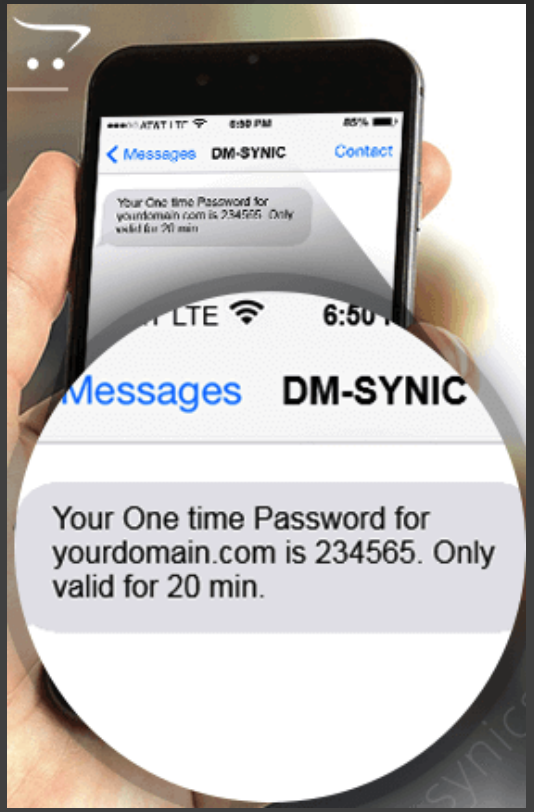
MFA Guidance

Knowledge-based authentication (KBA) is banned

- bad security
- bad usability

One-time password over SMS is restricted

- Public switched telephone network has extensive vulnerabilities



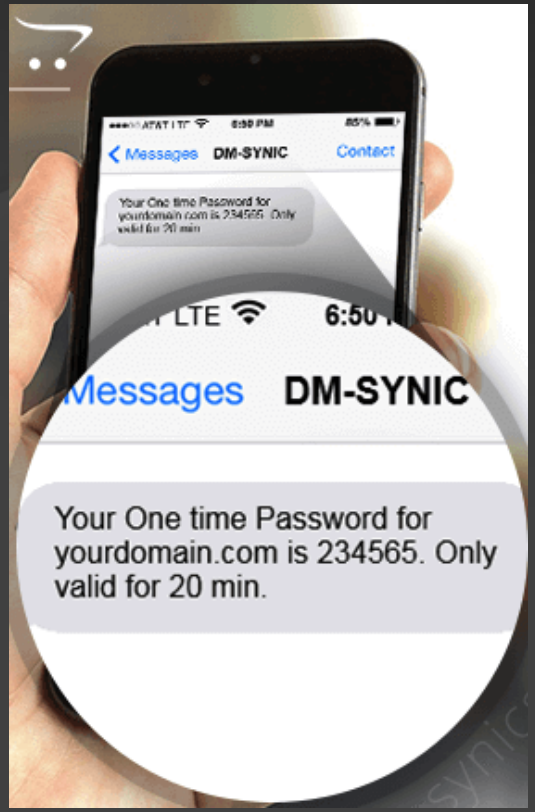
MFA Guidance

Knowledge-based authentication (KBA) is banned

- bad security
- bad usability

One-time password over SMS is restricted

- Public switched telephone network has extensive vulnerabilities
- SMS can be sniffed



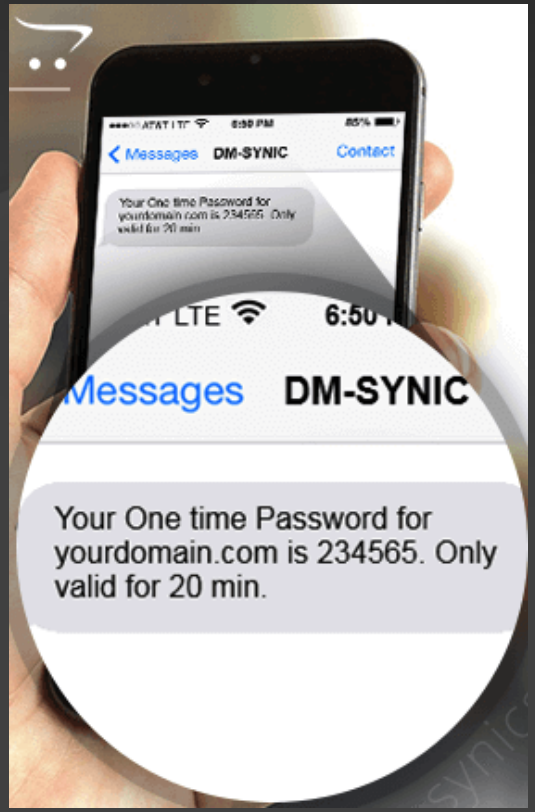
MFA Guidance

Knowledge-based authentication (KBA) is banned

- bad security
- bad usability

One-time password over SMS is restricted

- Public switched telephone network has extensive vulnerabilities
- SMS can be sniffed
- Easy to socially engineer phone number porting/device replacement



Password Policy Guidance

Special character requirements

Password Policy Guidance

Special character requirements

Forced rotation

Password Policy Guidance

Special character requirements

Forced rotation

Allow ridiculously long passwords

Password Policy Guidance

Special character requirements

Forced rotation

Allow ridiculously long passwords

Accept spaces and special characters

Password Policy Guidance

Special character requirements

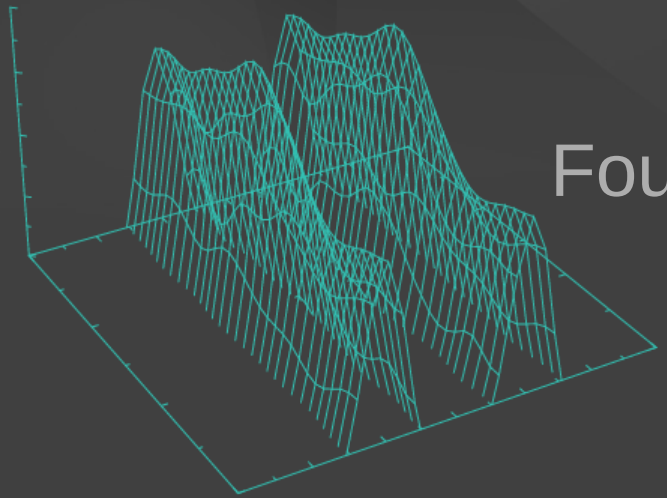
Forced rotation

Allow ridiculously long passwords

Accept spaces and special characters

Compare to breach corpus

Thank you



Sarah Squire
Founder and Principal Consultant
ENGAGE IDENTITY

@SarahKSquire