Scalable Authentication

Rolf Lindemann
Nok Nok Labs, Inc.
IT Has Scaled

Technological capabilities: (1971 → 2013)
Clock speed x4700
#transistors x608k
Structure size /450

Price: (1980 → 2013)
HDD $/MB /12k
NV RAM $/MB /1.3m

Ubiquity:
More than 7bn mobile connected devices by end of 2013

Connectivity: (2013)
34% of all people worldwide have internet access

Social media: (2013)
>10% of all people worldwide active

Relevance: (2012)
$1 trillion eCommerce
Authentication Hasn’t
Passwords

Too many to remember, difficult to type, and not secure

REUSED

PHISHED

KEYLOGGED
One Time Passcodes

Improve security, but not easy to use

- **SMS USABILITY**
  - Coverage | Delay | Cost

- **DEVICE USABILITY**
  - One per site | Fragile

- **USER EXPERIENCE**
  - User confusion

- **STILL PHISHABLE**
  - Social engineering
There are alternatives...
Implementation is the Challenge

Each new authentication solution requires new HW, SW, and Infrastructure.
⇒ We’re building ‘Silos’ of authentication
FIDO Goals

► Support for a broad range of authentication methods, leverage existing hardware capabilities.
► Support for a broad range of assurance levels, let relying party know the authentication method.
► Built-in privacy.
Abstract View

FIDO Authenticators

Mapping

FIDO SERVER
FIDO Functionality

- Discover supported authenticators on the client
- Register authenticators to a relying party (and bind it to an existing identity)
- Authenticate (a session)
- Transaction confirmation
Registration

FIDO CLIENT

Send Registration Request:
- Policy
- Random Challenge

Start registration

FIDO AUTHENTICATOR

Authenticate user
Generate key pair
Sign attestation object:
• Public key
• AAID
• Random Challenge
• Name of relying party
Signed by attestation key

FIDO SERVER

Verify signature
Check AAID against policy
Store public key

AAID = Authenticator
Attestation ID, i.e. model
Regarding AAIDs

**FIDO Authenticator**
- Using HW based crypto
- Based on FP Sensor X

**FIDO Authenticator**
- Pure SW based implementation
- Based on Face Recognition alg. Y

AAID 1

Attestation Key 1

AAID 2

Attestation Key 2
Privacy & Attestation

Bob’s FIDO Authenticator
Using HW based crypto
Based on FP Sensor X
Model A

FIDO SERVER RP1
Model A

FIDO SERVER RP2
Model A

Serial #
Authenticator Meta-Data

File available to FIDO Server with Authenticator descriptions

► AAID as an index
► Attestation trust anchor
► Implements Secure Display
► Key Protection
► ...

---

RSA CONFERENCE EUROPE 2013

Nok Nok LABS

#RSAC
Case A: Existing User

1. User A
   - Login with legacy credential

2. Authenticator 1
   - Perform FIDO Register function
Case B: New User

1. Create new account

User B

2. Perform FIDO Register function

Authenticator 2

Opt.: verify attrs. with 3rd party

User B

Authenticate 2

Cloud Service

Cloud Service

"Binding Authenticator to User"
Authentication

Send Authentication Request:
- Policy
- Random Challenge

Start authentication

Authenticate user
Sign authentication object:
- Random Challenge
- Name of relying party
Signed by authentication key for this relying party

Verify signature check AAID against policy
Transaction Confirmation

Like Authentication, but Authenticator displays Transaction Text

FIDO CLIENT

FIDO AUTHENTICATOR

Authenticate user
Sign transaction object:
• Random Challenge
• Name of relying party
• Transaction Text Hash
Signed by authentication key for this relying party

FIDO SERVER

Verify Transaction Text Hash
Verify signature check AAID against policy

Transfer $10000 to John Doe’s account 1234567
FIDO Building Blocks

- **FIDO USER DEVICE**
  - BROWSER / APP
  - FIDO CLIENT
  - FIDO AUTHENTICATOR

- **RELYING PARTY**

- **WEB SERVER**

- **FIDO SERVER**
  - FIDO Repository

**Diagram Components**

- **UAF Protocol**
- **TLS Server Key**
- **Cryptographic authentication key reference DB**
- **Authentication keys**
- **Attestation key**
- **Authenticator attestation trust store + meta data**
- **Update**

**Additional Details**

- **Cryptographic**
- **authentication key**
- **reference DB**
- **Authentication**
- **keys**
- **Attestation key**
- **Authenticator attestation trust store + meta data**
The Authenticator Concept

FIDO Authenticator

- User Verification / Presence
- Secure Display
- Attestation Key
- Authentication Key(s)

Injected at manufacturing, doesn’t change
Generated at runtime (on Registration)

User
Scalability of Authentication

- Scalable for Users
- Scalable User Verification Methods
- Scalable Assurance Level
Scalable for Users

Overall complexity doesn’t grow with the number of relying parties:

► Choosing & remembering one password per RP is not scalable
► Carrying one (dedicated) OTP token or smart card per RP is not scalable
► In FIDO, the Authenticator maintains one key per RP. This scales & avoid a global correlation handle.
Scalable User Verification Methods

Various User Verification Methods can be implemented without updating server software

► Various cryptographic hardware, e.g. smart cards, USB tokens, …

► All kinds of biometrics
  ► Fingerprints
  ► Face recognition
  ► Typing behavior
  ► Gait
  ► Cardiac rhythm recognition and more…

► Gadget presence, e.g. smart watch, …
Various User Verification Methods can be implemented without updating server software.
Scalable Security

Broad range of assurance levels

► Login to online account
  Low

► Change shipping address

► Transfer $10,000 to Account 1234
  High
Scalable Security (2)

Normal HW

Secure HW

Authenticator
User Verification
Crypto Layer

Authenticator
User Verification
Crypto Layer

Authenticator
User Verification
Crypto Layer
Scalable Security (3)

Scale the accuracy of the user verification algorithm, e.g. better finger print sensor/algorithm, longer PINs

Source: NIST Interagency Report 7477
Scalable Security (4)

Scale security by adding enhanced anti spoofing methods, e.g. enhanced liveness detection for face recognition. Or by requiring PIN entry.

Source: Liveness Detection for Face Recognition

Source: Live Face Detection Based on the Analysis of Fourier Spectra
FIDO and IAM

- Physical-to-digital identity
- User Management
- Authentication
- Federation
- Single Sign-On

Modern Authentication

Passwords

Strong

Risk-Based

RSACONFERENCE EUROPE 2013

#RSAC

Nok Nok LABS
Complementary

Who you claim to be

H3a4k
EXPLICIT AUTHENTICATION

Who you are deduced to be

IMPLICIT AUTHENTICATION
FIDO and Federation

First Mile

PASSWORDS

FIDO

Second Mile

SSO/FEDERATION

SAML

Google

Salesforce.com

OpenID

Concur

RSACONFERENCE EUROPE 2013

#RSAC

Nok Nok LABS
FIDO and Federation

FIDO USER DEVICE
- Browser/App
- FIDO Client
- FIDO Authenticator

IdP
- Id DB
  - Knows details about the Authentication strength

Service Provider
- Federation

FIDDBERVER
- OSTP
  - Federation

Knows details about the Identity and its verification strength.
FIDO Today

• **Technical Working Groups active**
  - Public Spec Drafts early 2014
  - Early Pilots late 2013
  - Complement existing standards & efforts
    - NSTIC/Federation: OpenID, SAML etc.

• **FIDO Alliance membership is growing**
  - Members set requirements and design the technology
    - Internet Services
    - Client Platform Owners
    - Device & Component Vendors

[info@fidoalliance.org](mailto:info@fidoalliance.org) | [www.fidoalliance.org](http://www.fidoalliance.org)
FIDO Alliance Members
## What’s the benefit

<table>
<thead>
<tr>
<th>For Users</th>
<th>For Internet Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Easy to use local auth options</td>
<td>• Greatly improved security, Increased user engagement</td>
</tr>
<tr>
<td>• No more worrying about passwords</td>
<td>• User brings own device</td>
</tr>
<tr>
<td>• Feel safer on the Internet</td>
<td>• Build server once: leverage all auth methods</td>
</tr>
</tbody>
</table>

**For Vendors**

- Standardization ignites market
- Solve fragmentation issues with unified framework
Backup
Summary

► Passwords don’t work
► Current alternatives don’t scale
► FIDO Alliance works on an open specification separating user verification method from cryptographic authentication protocol
► With that protocol
  ► relying parties can define policy for risk appropriate authentication
  ► relying parties know the authenticator model and its characteristics through attestation
  ► adoption of new authentication methods will be significantly easier
Thank you!

Rolf Lindemann
Nok Nok Labs, Inc.
rolf@noknok.com
www.noknok.com
www.fidoalliance.org
info@fidoalliance.org