

Beyond Passwords

Envision a world beyond password to improve user experience, security and efficiency in a digital world

2017 Fall MISA Conference

By

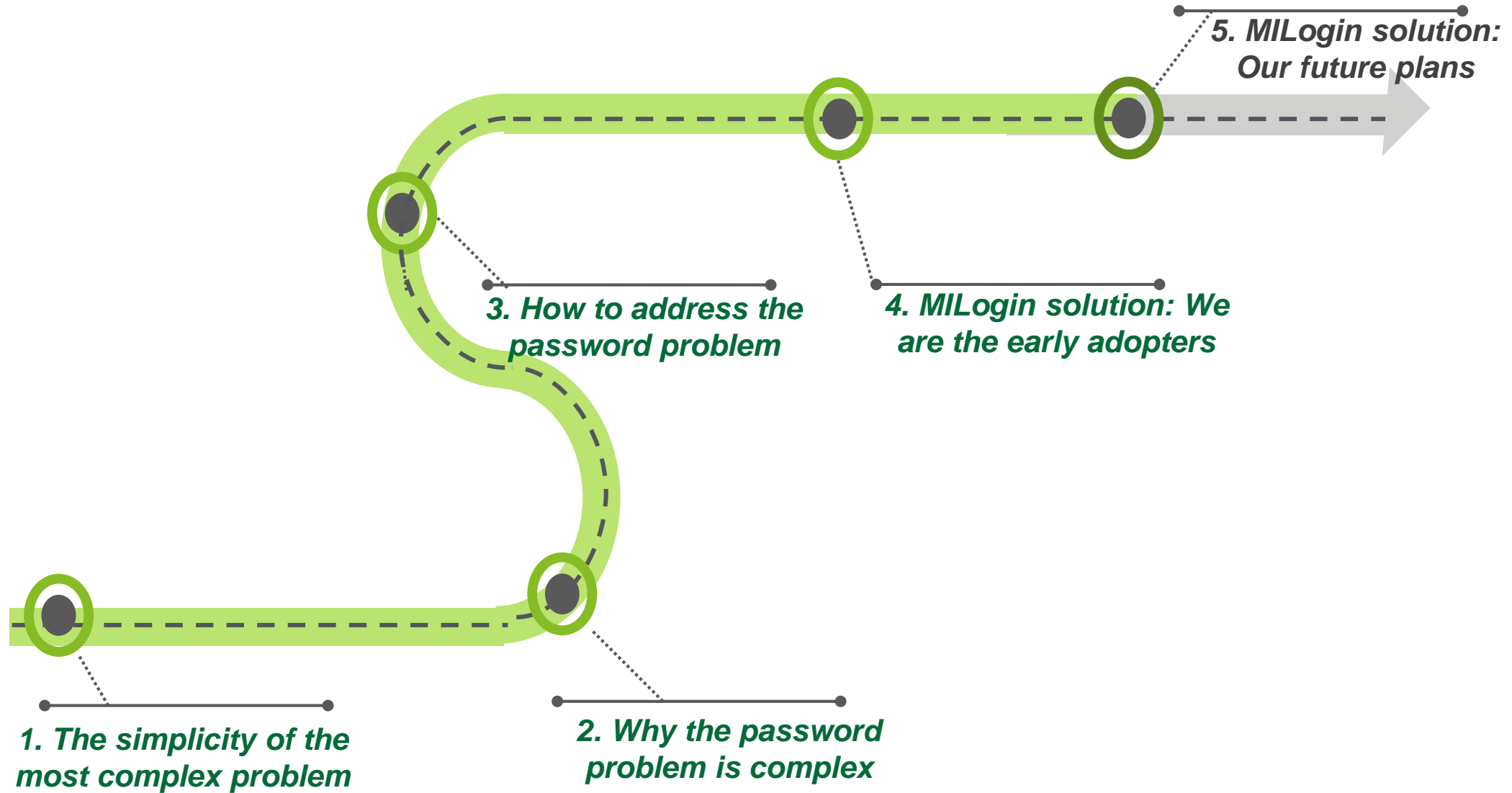
**Manish Amlathe,
Rohit Singla**

9/21/2017

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.



Session objectives



The simplicity of the most complex problem

Better forms of authentication have been available for years — so why are we still using passwords?

- **Our experiences with IT begin with a transaction that's both annoying and, in terms of security, one of the weakest.**
- **Paradoxically, the password solutions continue to appeal due to ease of deployment, lower cost and intuitiveness.**

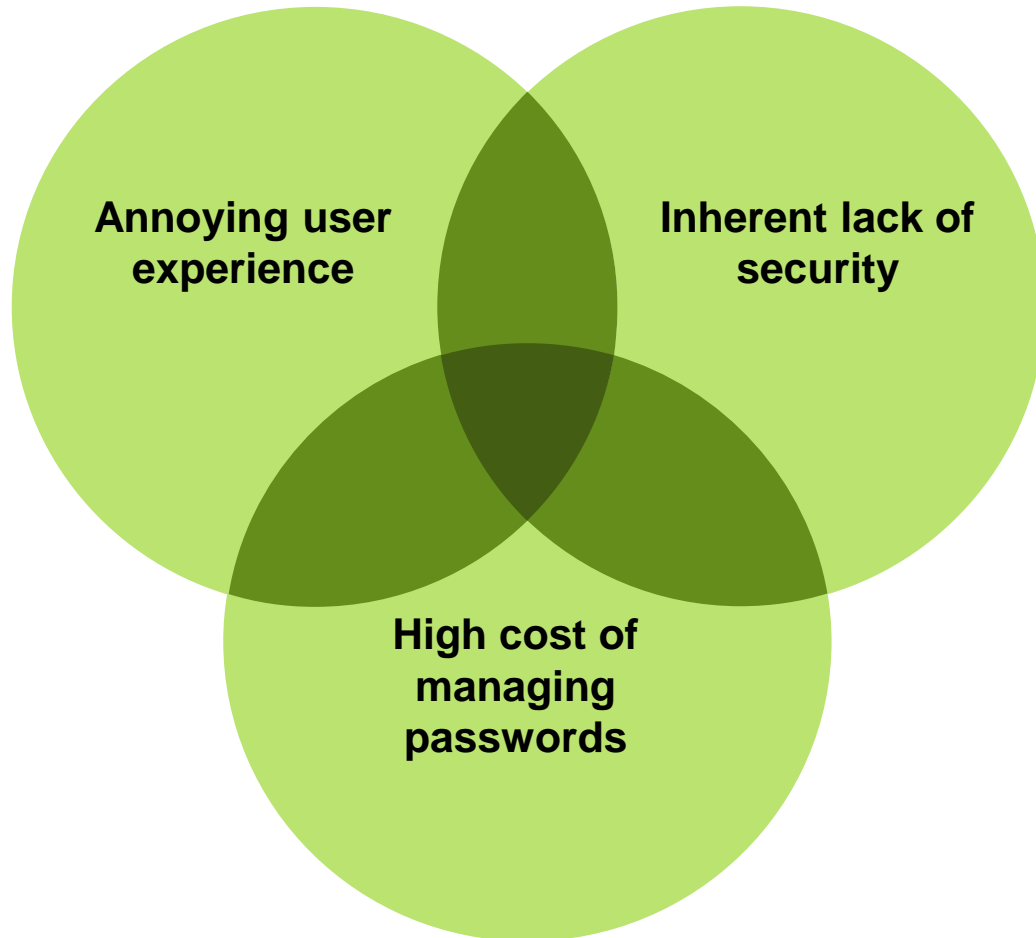
- Passwords have been a cornerstone of the information age, serving as our digital keys for the last 50 years allowing users to represent “something you know” of the MFA.
- In spite of the predictions that “the password is dead” and efforts to replace them passwords still appear as the dominant form of authentication on the Web.
- Password based authentication is an essential element of modern IT systems, yet understanding options and balancing requirements remain complex.

Note: Although the terms "identification" and "authentication" are often linked, they aren't synonymous from a security perspective. Identification usually comprises a string (such as a username) authentication is the process of determining whether an identified user is truly the person he or she claims to be

Why the password problem is complex

Hackers have gotten very good at what they do:

- With more capable tools than ever, and those tools can work so well because;
- We are still really bad at choosing and remembering passwords.



User Experience

- Difficult to remember and easy to guess
- User fatigue with password lock, recovery and profile
- The enormity of number of passwords

Security

- Technology and social venues to hack
- Password strength v/s value of data/transaction
- Password reuse and false sense of security

Cost and Impact

- Operations and password reset cost
- Integration/technology cost
- Average cost and impact of breach

How to address the password challenge: The approach

Planning “Beyond passwords” may sound daunting, requiring major IT upgrades, but organizations can take incremental steps.

Incremental Steps

1. Assess business priorities and identify weaknesses in the authentication system

2. Examine practical, cost-effective, and scalable authentication solution

3. Conduct a pilot in high-priority business operations

4. Expand the solution to a wider set of operations in phases based on priority

Considerations for Authentication Solution

- Enterprises should evaluate password solution on three scales:
 1. User Experience (e.g., need not to remember, nothing to carry, easy to use)
 2. Security (e.g., Resilient to physical and logical guess and impersonation)
 3. Ease and cost of deployment (e.g., low cost, compatibility)
- Implement flexible risk-based approach where user authentication is commensurate with the value of the transactions

How to address the password challenge: The options

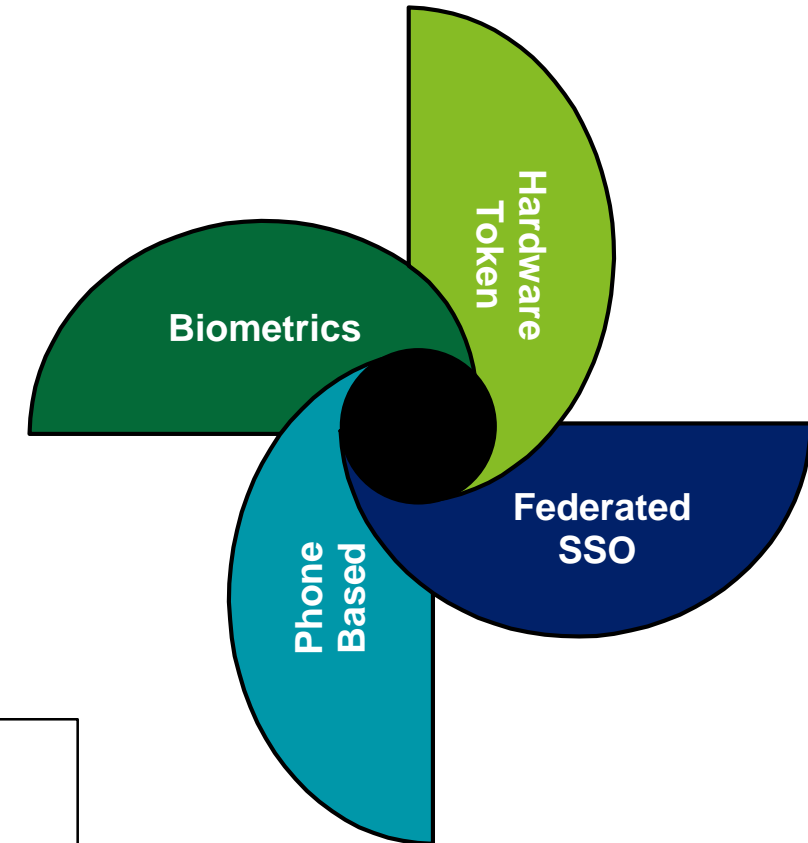
Passwords are going to be replaced by...you or devices you carry. Your mobile, face, fingerprints, even your iris will authenticate your entry into the digital world.

Authentication usability framework*

Factors	User Experience Score	Security Score	Ease and cost of deployment score
Passwords	Low	Low	Low
Biometrics	High	High	High
Hardware Token	Low	Medium	Medium
Federated SSO	Medium	Medium	Low
Phone Based	Medium	Medium	Medium

With a quick glance on the table above:

- Most factors do better than passwords on security
- Every factor performs equal to or worse than passwords on deployment ability








*The authentication usability framework needs to be evaluated for the actual rating and score against various factors and underlying technology mechanism. The rating specified above is for illustrated purposes only.

** Federated SSO mechanism will rely on the authentication mechanism of the provider

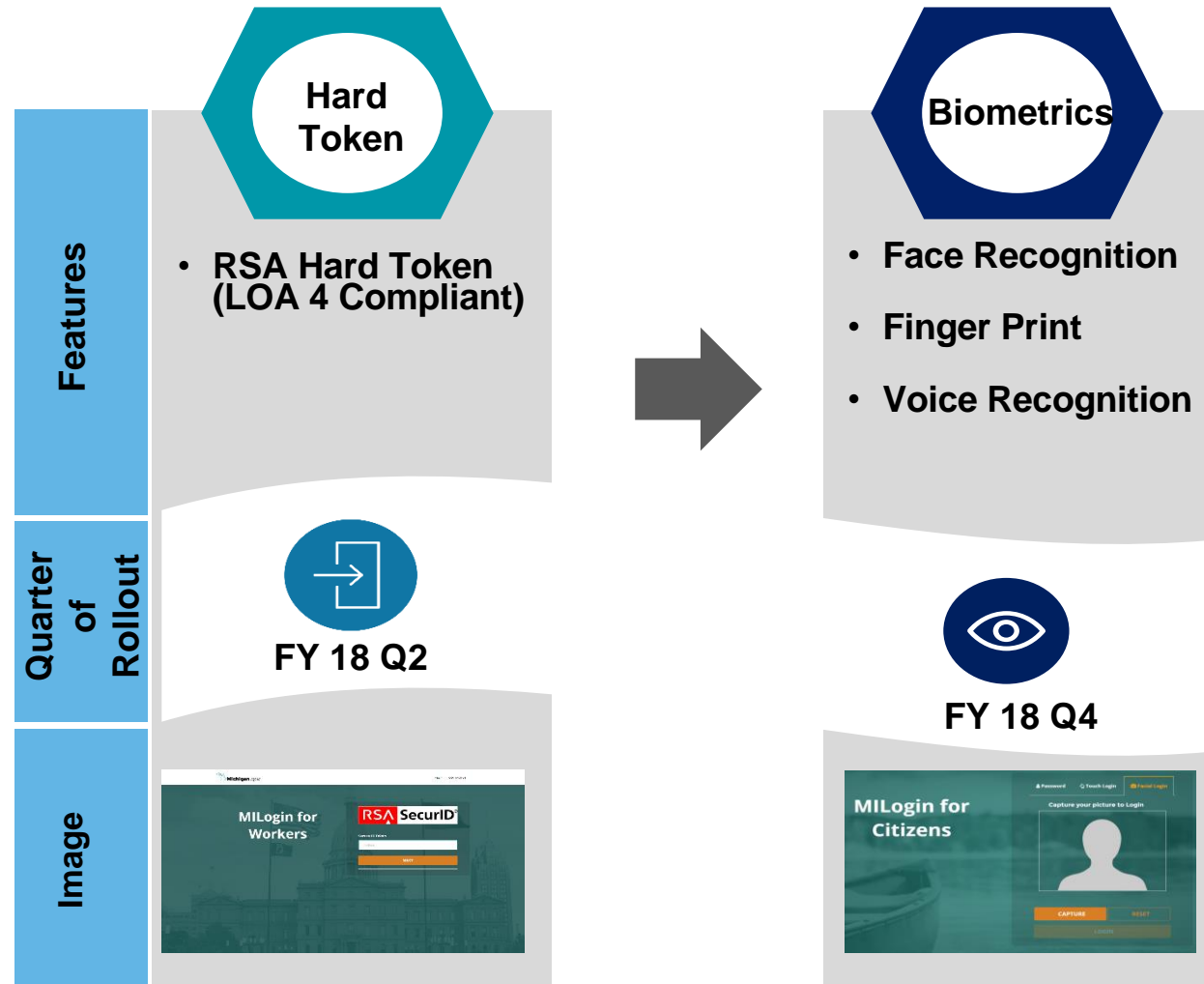
MILogin solution: We are the early adopters

MILogin is an Enterprise Identity, Credential, and Access Management (ICAM) solution of the State. Today over 700,000 business entities, 70,000 state employees and contractors, and 130,000 citizens are using MILogin to access more than 170 applications across 13 state agencies.

 Services/ Business Functions	 Key Features
Federated Single Sign-on 	<ul style="list-style-type: none">• Single sign-on (Seamless Login)• SAML 2.0 based integration• Desktop SSO for SOM AD based workers
Mobile Based 	<p>Options supported by MILogin:</p> <ol style="list-style-type: none">1. One-time password (OTP) via Text,2. Phone call back3. Soft Token / Mobile application,4. OTP via email
Application Account management 	<ul style="list-style-type: none">• Automated user account management to applications

MILogin solution: Our future plans

By the end of FY18, over 4 million users will leverage MILogin to enhance user experience, improve security and drive operational efficiencies



Contact information

Manish Amlathe

Phone: (517) 775-1067

Mail: mamlathe@deloitte.com

Rohit Singla

Phone: 401-219-0335

Mail: rosingla@deloitte.com

Amit Aurora

Phone: (517) 242-0328

Mail: auroraa@michigan.com

Scott Flagg

Phone: (517) 898-6315

Mail: flaggs@michigan.gov

Q&A

Key references

- A world beyond password: By Mike Wyatt, Irfan Saif, and David Mapgaonkar
- The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes by Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano