Identity Proofing and NIST SP 800-63: Applications in Healthcare

May 10, 2011

Agenda

- OMB M-04-04 and NIST 800-63 Overview
- Experian and Symantec
- Risk-Based Authentication and ID Proofing
- Case Studies
  - SSA
  - DrFirst
- Summary

OMB M-04-04 E-Authentication Guidance

- Electronic authentication (E-Authentication) is the process of establishing confidence in identities presented remotely over an open network to an information system.

- OMB M-04-04 defines four levels of identity assurance for electronic transactions requiring authentication, where the required level of assurance is defined in terms of the consequences of authentication errors and the misuse of credentials.

    - Level 1 – Little or no confidence in the asserted identity
    - Level 2 - Some confidence in the asserted identity
    - Level 3 - High confidence in the asserted identity
    - Level 4 - Very high confidence in the asserted identity

OMB M-04-04 E-Authentication Guidance

- Requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.
  1. Conduct a risk assessment of the online system.
  2. Map identified risks to the applicable assurance level.
  3. Select technology based on e-authentication technical guidance.
  4. Validate that the implemented system has achieved the required assurance level.
  5. Periodically reassess the system to determine technology refresh requirements.

Mapping Impact to Applicable Assurance Level

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

NIST Special Publication SP 800-63-1
Electronic Authentication Guideline

- A companion to OMB M-04-04, which provides *technical* guidelines for Federal agencies to allow an individual to remotely authenticate his/her identity over an open network to a Federal IT system.
- NIST SP 800-63 defines technical requirements at the four assurance levels in the areas of :
  - identity proofing and registration
  - tokens
  - management processes
  - authentication protocols
  - assertions

Multi-Factor Authentication

A combination of two or more authentication factors (tokens)

Something You Know

Username/Passwords
Mother's Maiden Name

Something You Have

Hardware OTP Token
Digital Certificate
Smart Card

Something You Are

Fingerprint
Iris Pattern

NIST SP 800-63 Technical Guidelines

Levels 1 - 4	Technical Guidelines
1. Little or no confidence that the asserted identity is valid.	▪ Identity Proofing *not* required ▪ Single Factor Authentication ▪ PIN or Knowledge-based Password
2. Some confidence that the asserted identity is accurate.	▪ Online verification of identity elements. ▪ Single Factor Authentication ▪ PIN or Knowledge-based Password
3. High confidence that the asserted identity is valid.	▪ Identity proofing either *in-person* or *online* ▪ Online verification of identity elements *and* financial account information ▪ Multi-Factor Authentication
4. Very high confidence that asserted identity is valid.	▪ PKI digital signature ▪ Biometrics ▪ Multi-factor Hardware token

Experian/Symantec Partnership

- Experian is an industry leader in Fraud and Identity Verification solutions, with comprehensive consumer and business databases.
- Symantec is a certified provider of authentication solutions for Federal government agencies and organizations needing to interoperate securely with the Federal government.
- Symantec provides both managed Public Key Infrastructure (PKI) services and in-the-cloud One-Time-Password Validation services supporting multiple hardware and software token types.
- Experian and Symantec have collaborated to provide a comprehensive suite of identity proofing and authentication services that supports the National Institute of Standards and Technology's (NIST) Electronic Authentication Guideline (Special Publication 800-63).

Risk-Based Authentication and ID Proofing Overview

IDENTITY PROOFING AND NIST SP 800-63: APPLICATIONS IN HEALTHCARE

What and why risk-based authentication?

- Definition
  - Holistic assessment of a subject and transaction with the end goal of applying proportionate authentication and decisioning treatment
- Core value propositions
  - Efficiency in process and transactional cost
  - Risk-assessment performance lift over traditional binary rule sets and policies
  - Customer / subject user experience
  - Evolutionary adoption of emerging technologies and data assets
  - Flexibility and interoperability with core platforms and third party partners

What and why risk-based authentication?

Widely-adopted as a best practice in account opening and account management markets

- Card issuers
- Demand deposit accounts
- Personal loans
- Mortgage

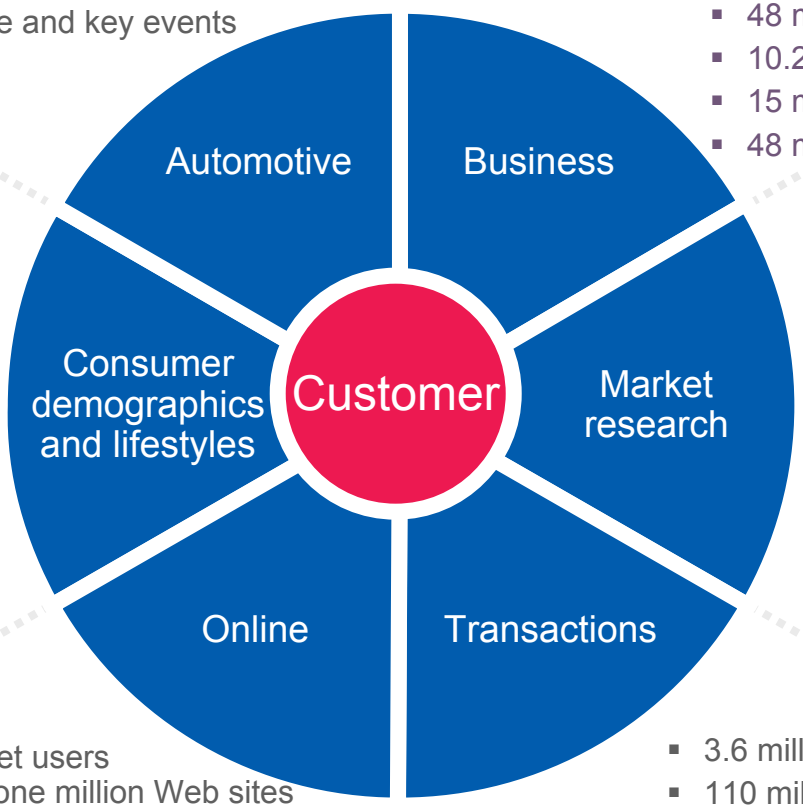
Gaining broader acceptance

- eGovernment
- Automotive
- eCommerce
- Telecommunications and utilities
- Healthcare

Comprehensive data to enable on-line ID Proofing
Unparalleled depth and breadth of information

- 425 million vehicles in U.S. & Canada
- Title, registration, mileage and key events

- 27 million active companies
- Greater than 100 million credit lines
- 48 million public records
- 10.2 million collection experiences
- 15 million tax identification numbers
- 48 million SIC codes



- 235 million consumers; 113 million households
- 1,000 demographic attributes
- 3.2 million births annually
- 16 million moves annually
- 20 million new homeowners
- 3,200 public and proprietary sources
- 100 million subscriptions
- 650+ psychographics

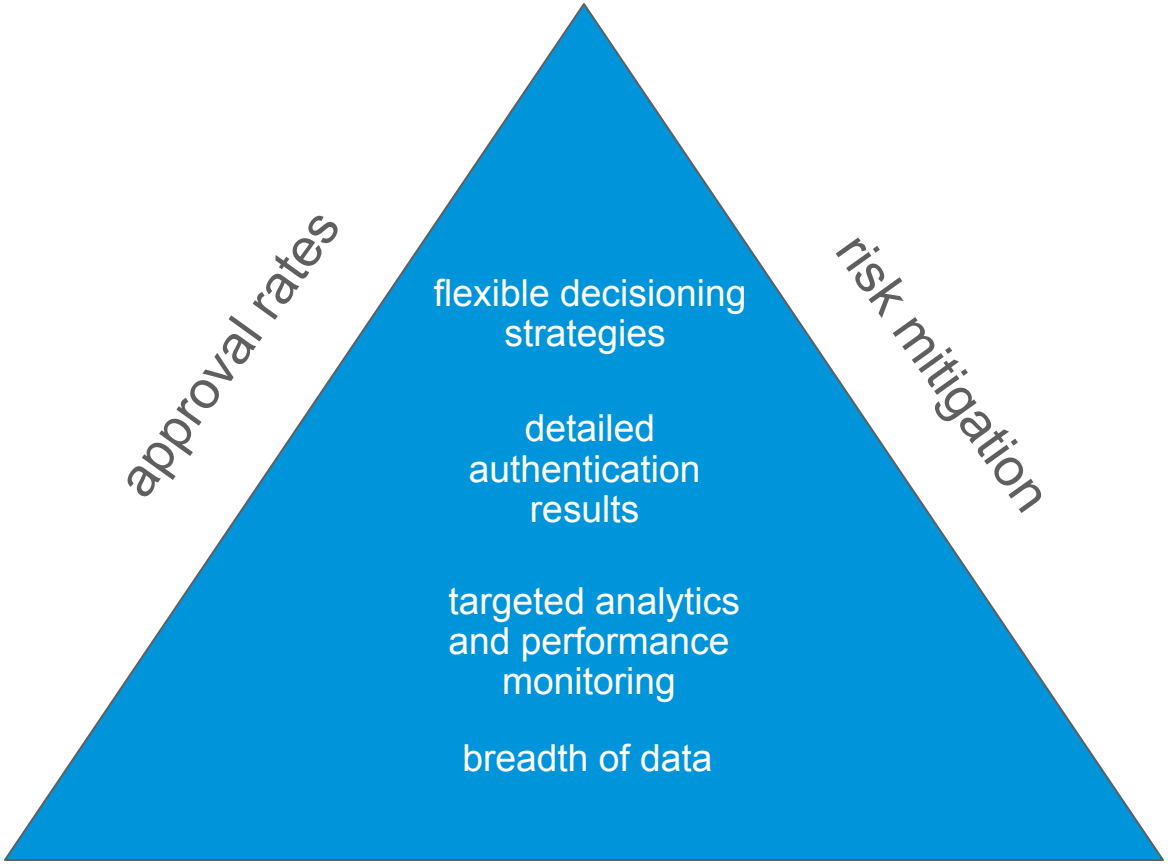
- Syndicated research: 30,000 consumers annually; 60,000 data variables
- 35 million double opt-in consumer panel 8,000 brands; 450 product categories
- Media viewer-ship across all media

- 25 million Internet users interacting with one million Web sites
- 15 million email addresses

- 3.6 million businesses
- 110 million catalog buyers
- 61 million magazine subscriptions

Balance competing forces and resource constraints
Calibrate via detailed output and decisioning

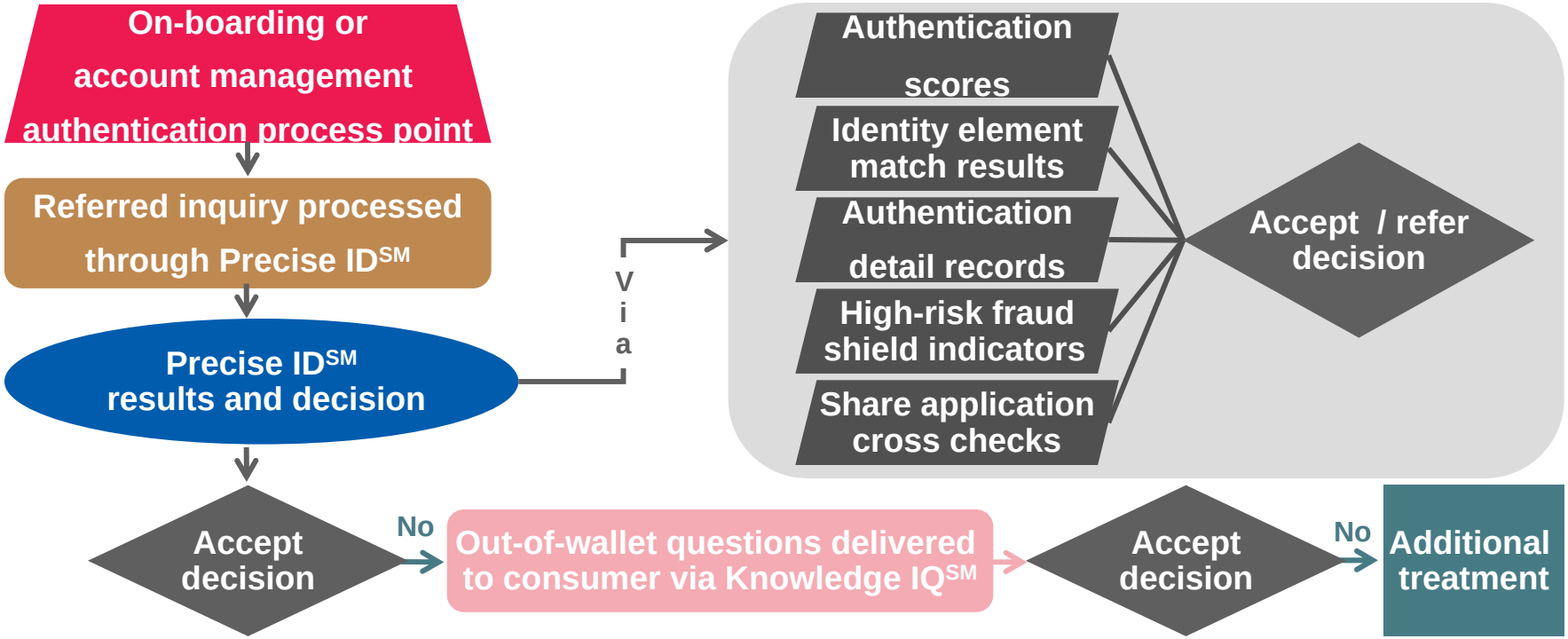
'More dials to turn'



Compliance *(NIST 800-63)*

Broader risk-based strategy

KBA as part of an overall fraud process, aiding in both preventing fraud and reducing manual intervention



Process on-boarding and transaction request
Precise ID℠ and Knowledge IQ℠ results archived and monitored for performance

SSA Case Study

IDENTITY PROOFING AND NIST SP 800-63: APPLICATIONS IN HEALTHCARE

SSA Case Study
Overview

SSA has an internal goal of increasing access of information and services via on-line channel to relieve increasing load on phone and field office resources.

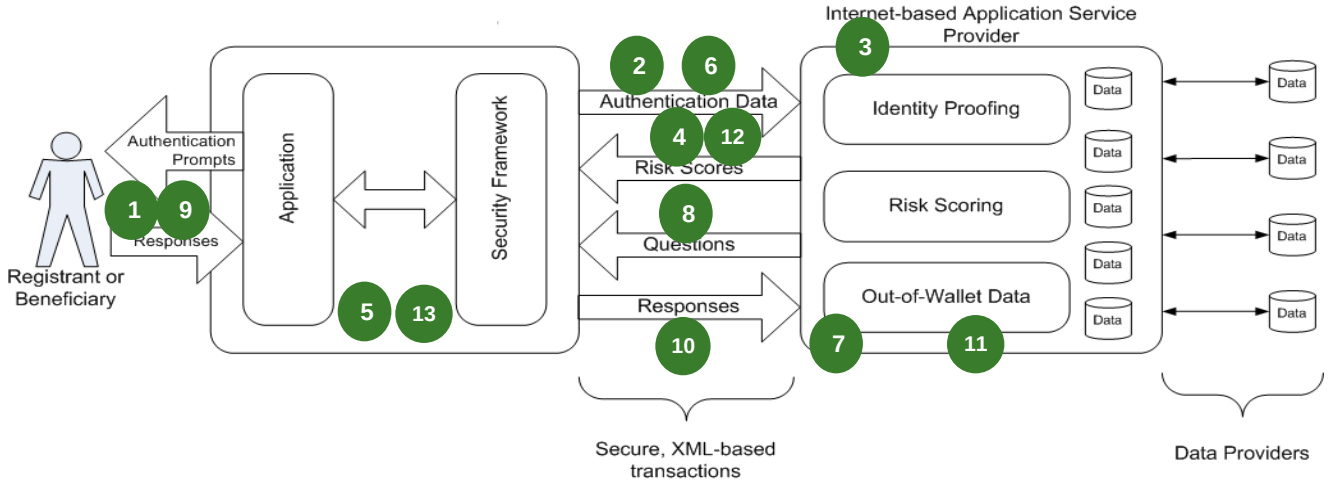
- ID Proofing of individuals required for SSA on-line account
- SSA leverages internal data sources and processes
- Experian e-Authentication will augment current SSA processes as part of new initiative
- Risk based approach utilizing Precise ID and Knowledge IQ

SSA Case Study
Experian and SSA

Experian and SSA continue to work collaboratively towards definition, development and integration of optimal ID proofing solution. Efforts include:

- Consulting support on cross-industry best practices and adapting them for SSA needs
- Focus on Level 2 and Level 3 NIST requirements
- Custom development to support specific SSA requirements
- On-going performance monitoring and continual process improvement

SSA Case Study
E-Authentication Two-Factor Work Flow



1. User enters name, address and credit card number
2. Input data passed to Precise ID & Credit Card Verification
3. Precise ID authenticates & verifies credit card
4. Results passed to Agency application
5. Solution evaluates results, passes user based on decision criteria
6. If decision to proceed to OOW question, send request to Knowledge IQ
7. KIQ generates OOW questions
8. Questions passed to Agency application
9. User is prompted to answer questions
10. If Solution passes question response to Knowledge IQ
11. Knowledge IQ evaluates the answers
12. Knowledge IQ passes result to Agency application
13. Solution evaluate results, passes or fail user

DrFirst Case Study

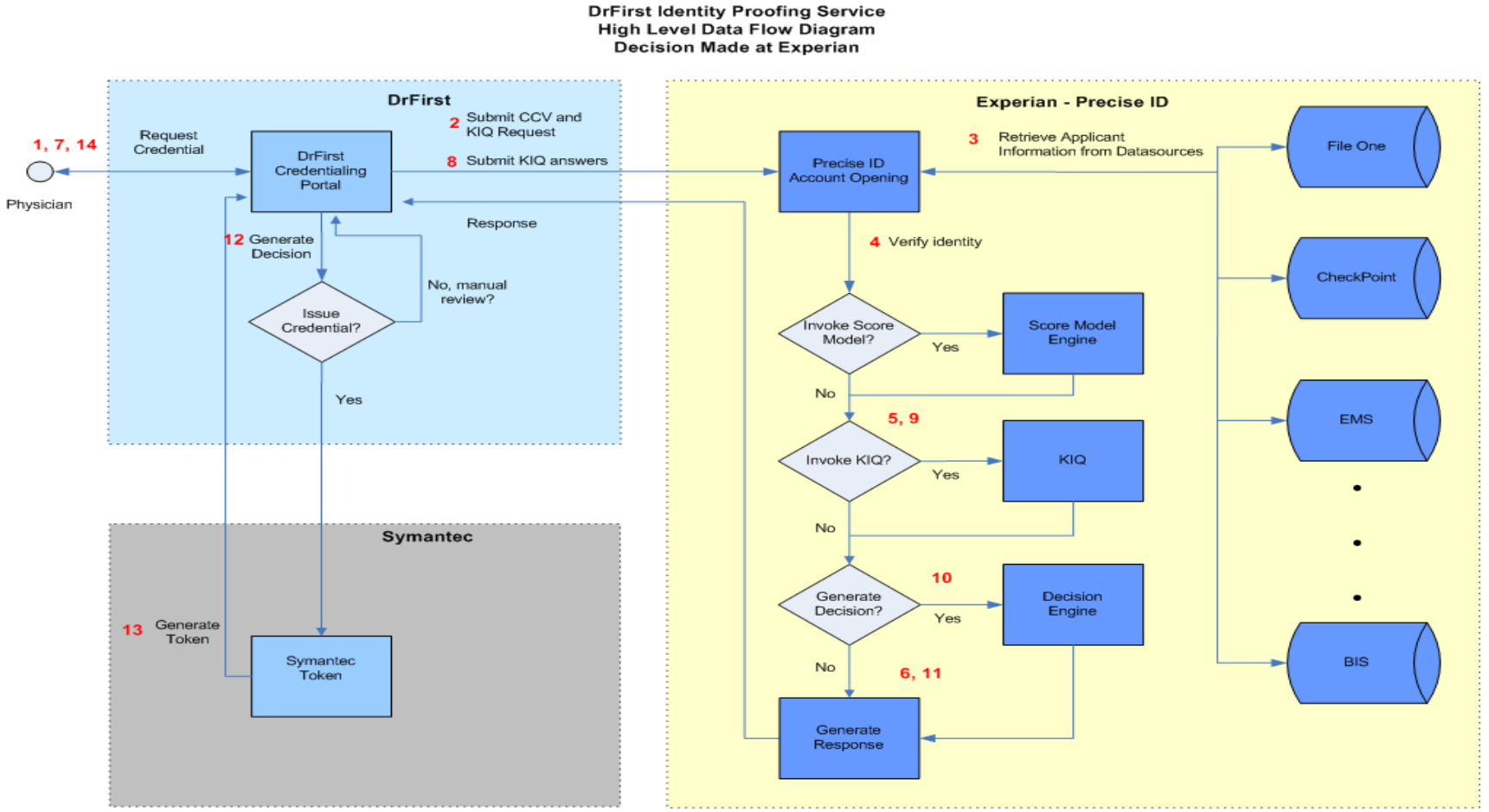
IDENTITY PROOFING AND NIST SP 800-63: APPLICATIONS IN HEALTHCARE

DrFirst Case Study
Overview

DrFirst had a need for a two-factor authentication solution which meets NIST SP 800-63-1 assurance requirements and Drug Enforcement Administration regulations.

- ID Proofing of physicians for ePrescribing eligibility
- DEA requires level 3 NIST assurance
- Experian and Symantec partner to provide two-factor authentication solution to meet NIST level 3
- Risk based approach utilizing Precise ID, Knowledge IQ, financial account verification and OTP

DrFirst Case Study
Experian, Symantec and DrFirst



DrFirst Case Study
Experian, Symantec and DrFirst

- Experian and Symantec continue to work collaboratively with DrFirst to provide:
  - Consulting support on cross-industry best practices and adapting them for DrFirst needs
  - On-going performance monitoring and continual process improvement
- ***This process will deliver a reusable NIST Level 3 identity authentication solution for healthcare and other applications!***