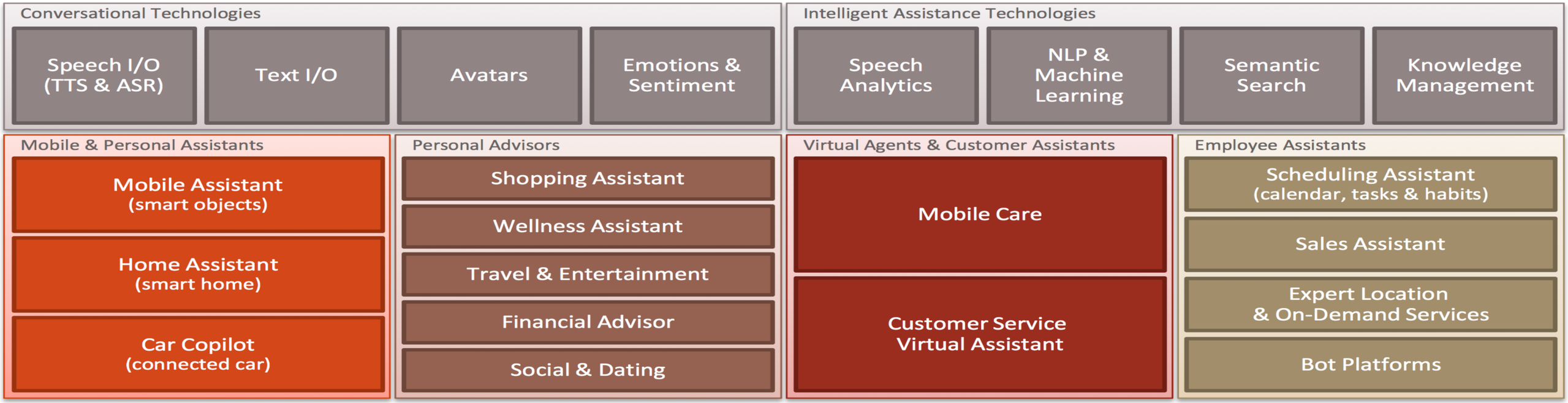
opusresearch

Building Specifications for Secure Intelligent Assistants

Presented by:
Dan Miller
Lead Analyst, Opus Research

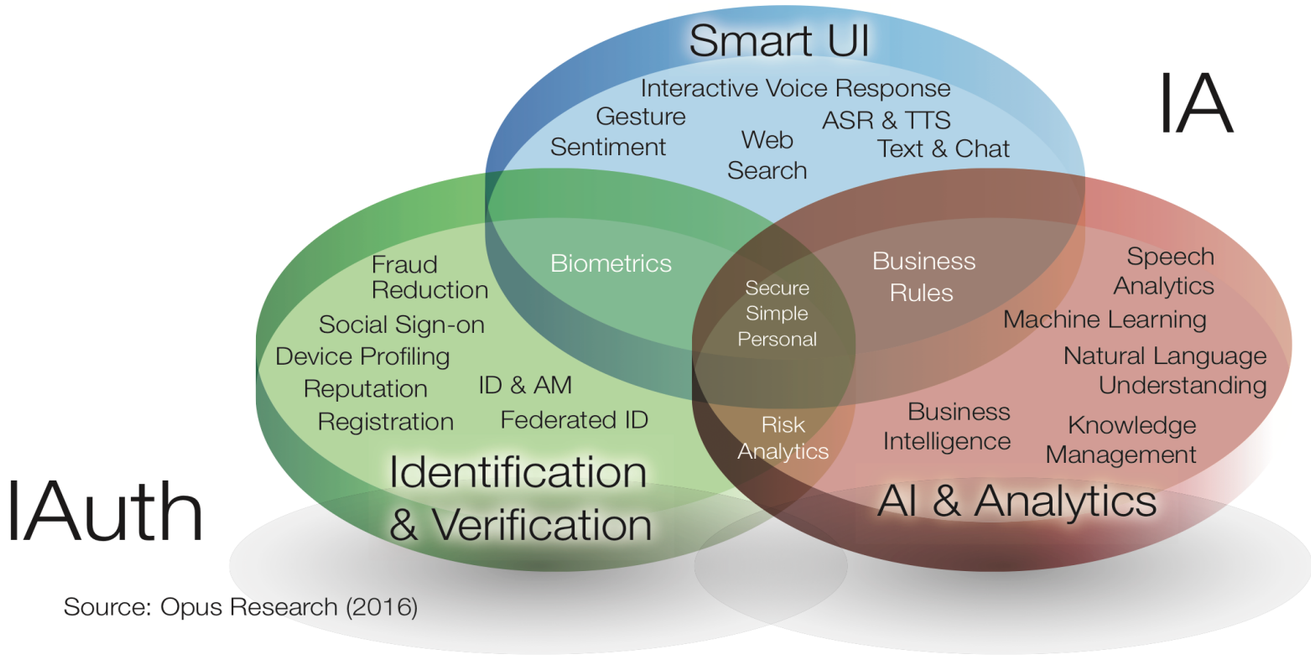
The IA technology stack

Smart UI + Natural Language + AI = Superior Customer Experience



Begs for better authentication

- Continuous
- Conversational
- Risk-Aware
- Multi-layered
- Multi-factor
- Integrated
- Biometric



Source: Opus Research (2016)

Change agents

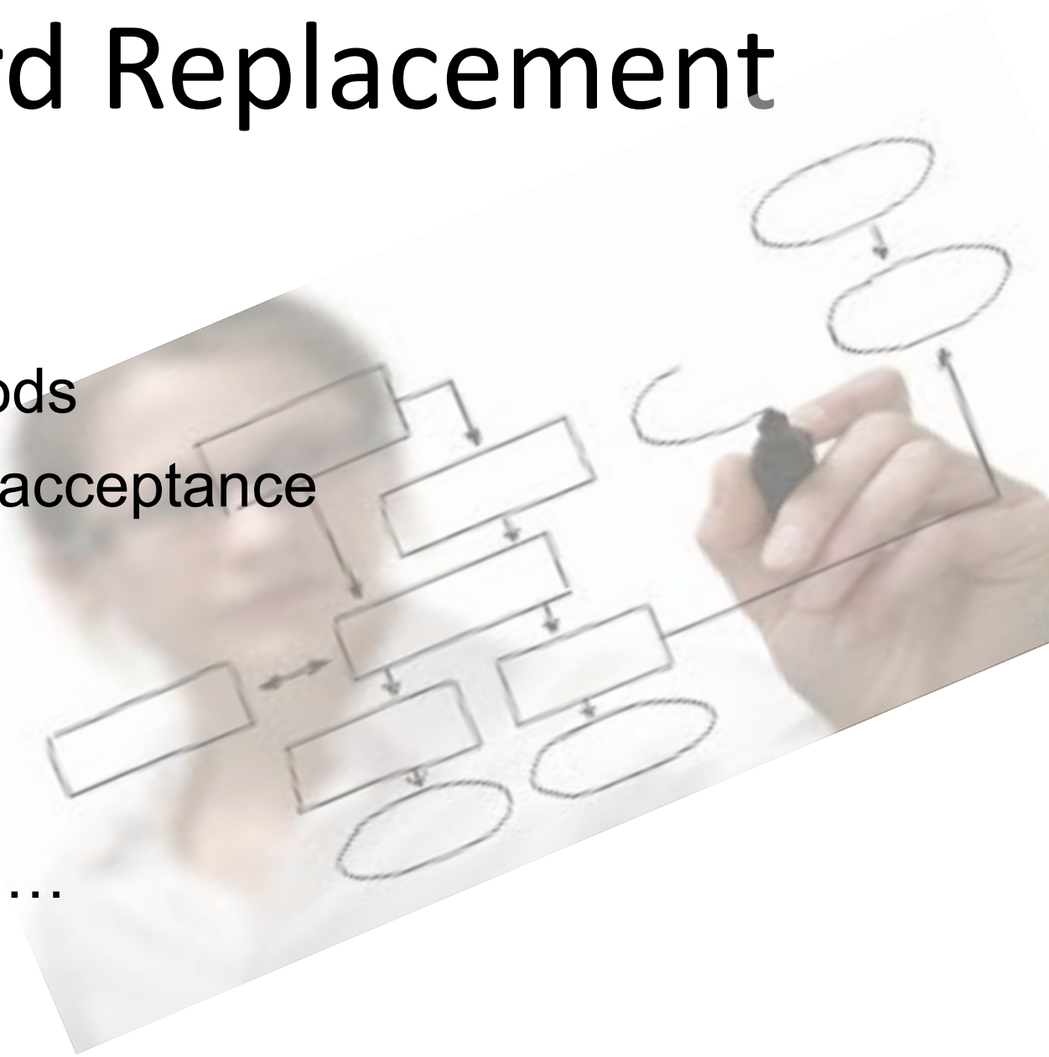
- Password and PIN replacement
- Security threats
- Fraud loss
- Customer experience
- Convenience
- Growth of Mobile and Omnichannel
- Personalization

Why now?

- Core technologies work
  - Proven accuracy and efficacy
  - Operates at scale
  - Integrates well with IT, security, CCTR, Web
- Organizations are VB & IAuth ready
  - Learned from ‘best practices’
  - Fits with agent workflows
  - Balances Security with CX

Moving Beyond Password Replacement

- PINs and passwords will be here forever
  - Augment and supplement current methods
  - Pay close attention to user comfort and acceptance
  - Match security to level of risk
- Leverage existing security infrastructure
  - More than simply replacing passwords
  - ID&AM, risk engines, intrusion detection…
  - Make customer experience paramount



Multi-layer, Risk-Aware Approach

- Simplicity masks complexity
  - Security baked into UX
  - Continuous scoring of risk levels
  - Application of multiple factors
- Benefits are measurable
  - Imposter detection
  - Fraud loss reduction
  - Less “social engineering”

Candidates for Standards

- FiDO Alliance
  - Supports hardened endpoints
  - On-device “matching”
  - Password-less user experience
- Alternative approaches
  - OAuth
  - SAML
  - OpenID
  - Social Sign-on

Focus on User Experience

- A multi-disciplinary effort
  - Involves CISO, CMO, CXO
  - Balances convenience and security
- Focus on personalization
  - Aware of user history and entitlements
  - Authenticates in the course of conversation