

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: IDY-R01

Operationalizing Identity: IAM for Customer Service

Arynn Crow

Manager of Product Management
AWS

Twitter: @arynncrow

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

A smiling woman with curly hair, wearing a headset and a white shirt, is in the foreground. She is looking slightly to the right. In the background, two other people are also wearing headsets and working at their desks. The setting appears to be a call center or a customer service office. The lighting is warm and bright.

Welcome!

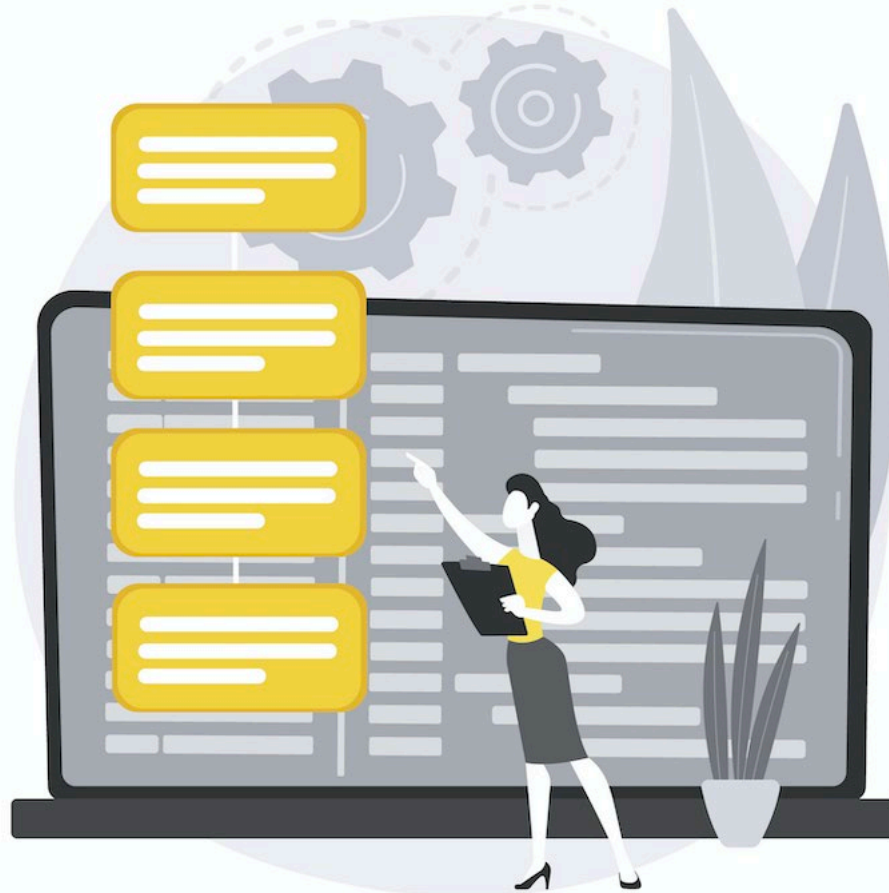


So, what are we doing here?

We'll cover...

- Common use cases and risks (why this environment matters in security & identity)
- Customer versus workforce considerations
 - Help desk may overlap, but not explicitly covered
- How to distill these considerations into a plan

I. Use Cases and Risks



The Customer Service Landscape

- Customer service ecosystem is often a call center, but can be anywhere your customer is interfacing with your organization
- Customers have high expectations, and agents have advanced capabilities to meet those expectations
- High expectations, but communication channels are limiting

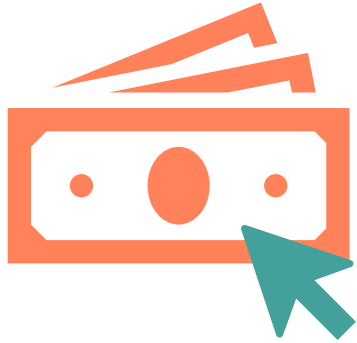
Common Use Cases

- Seemingly innocuous and transactional – where's my order, replacements
- Help with compliance and data requests
- Configuration help for user or business accounts
- Modifying critical account information – including, when self-service fails, account recovery

Many Use Cases, More Data Access

- Access to PII, such as...
- Payment and billing data
- Social security numbers, birth dates
- Personal documents – utility bills, driver's licenses, bank statements, etc.

Agents May Have Advanced Privileges



- Add, change, remove payment & billing information



- Modify user credentials

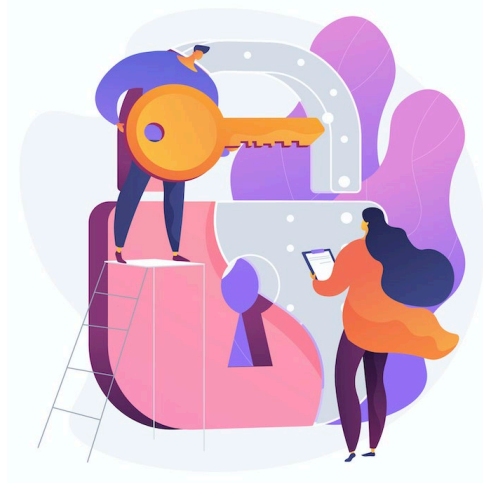


- Change account state or suspend account/service



- Place orders, take other actions on customer's behalf

Your objectives are...



Prevent Account Takeover and Fraud

- Humans are biased to empathy
- Social engineering is increasingly common
- Customer service is the most visible human interface



Prevent Data Exposure

- Monitor and minimize internal and external access
- Customers in different demographics can have different data sensitivities

II. Considerations for Customers and Workforces

#RSAC



Customers



Workforce

Authentication

- Agents determine that customers are who they say they are – this is the primary or only defense for many organizations
- Familiar authentication challenges are complicated by channel –sign-in portal protections may be unavailable
- Customers expect help from anywhere any time. This creates tension between security and satisfaction



Adapting to the channel



Knowledge-Based Authentication

- Certain attributes are easily discoverable, or immutable
- Persists due to ease of use – no equipment needed



Pins and Passwords

- May or may not be specific to customer service.
- Easy, but customers reuse these, and actors may replay them

PIN

- 931234

Passphrase

- ilovemydog2022

SMS and E-mail OTP

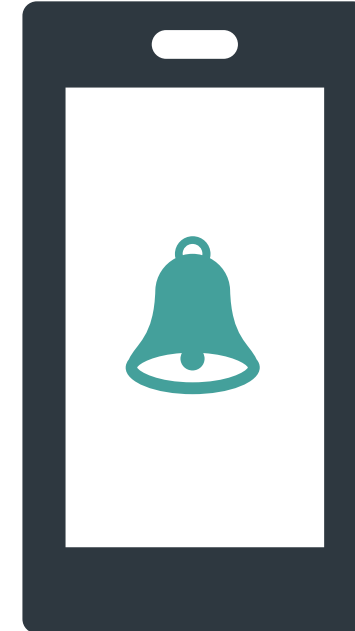
- Persists due to ease of use and wide adoption of mobile devices.
- May provide incremental assurance over KBA in certain cases

Your sign-in code for lovesdogs.com is 697830. This code will expire in 5 minutes.



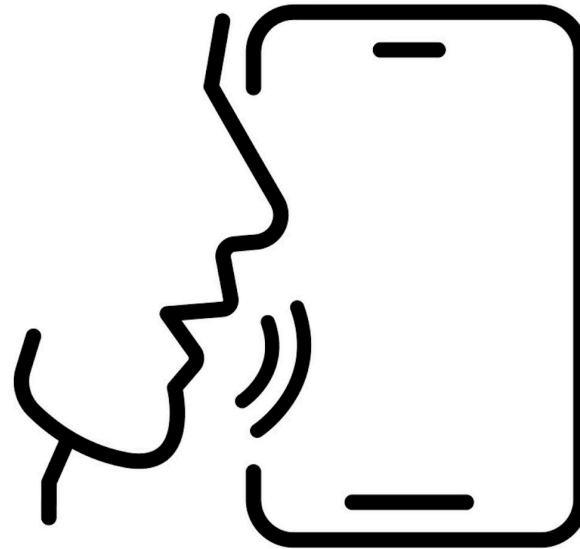
Push Notifications

- Easy to use. May also benefit stronger sign-in protections from a mobile app
- Requires well-adopted mobile app and connectivity



Voice Biometrics

- Easy to complete, relatively high assurance, fast and low-friction
- Privacy and implementation considerations add complexity

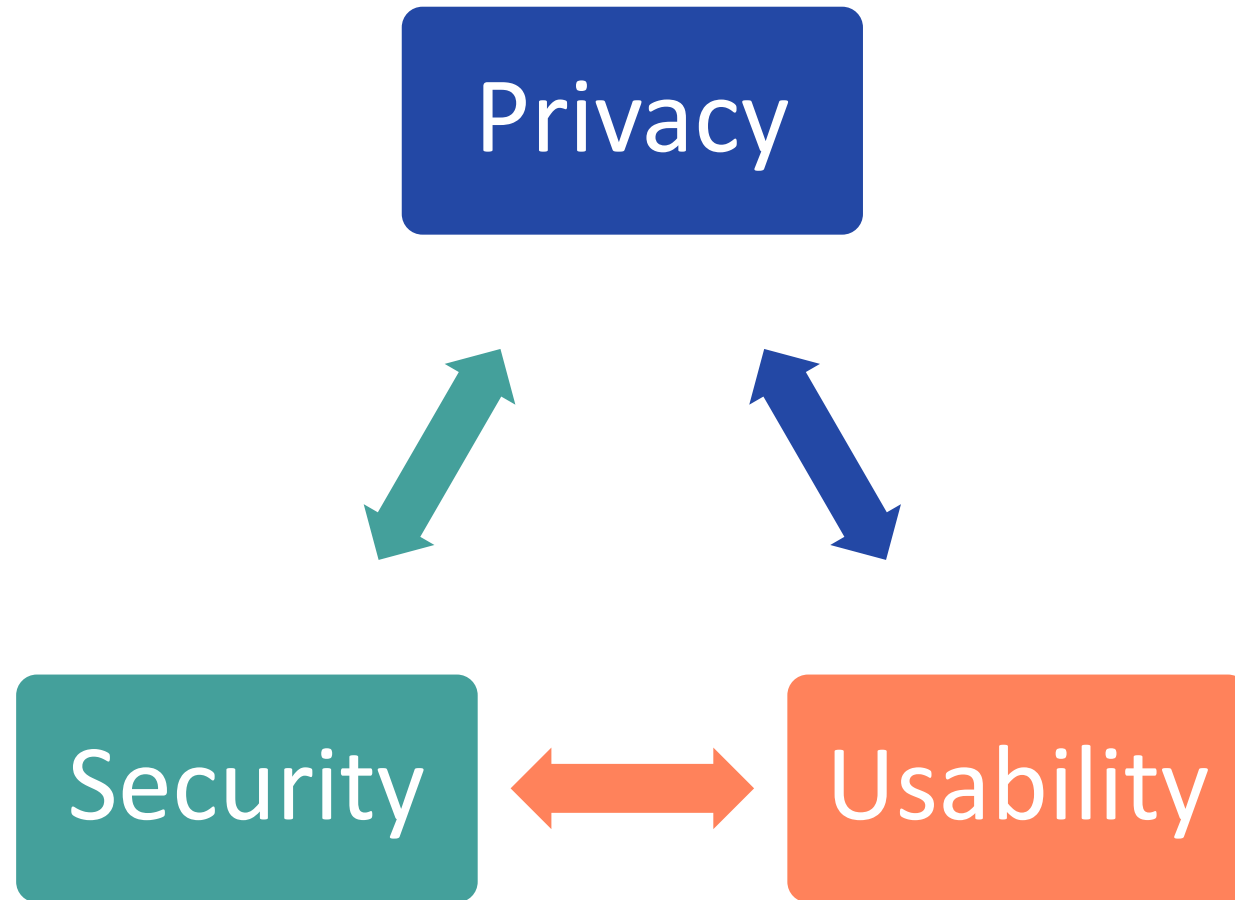


Browser Sign-In

- More limited use cases
- Benefits from full controls of your authentication stack.
- Won't work for recovery!

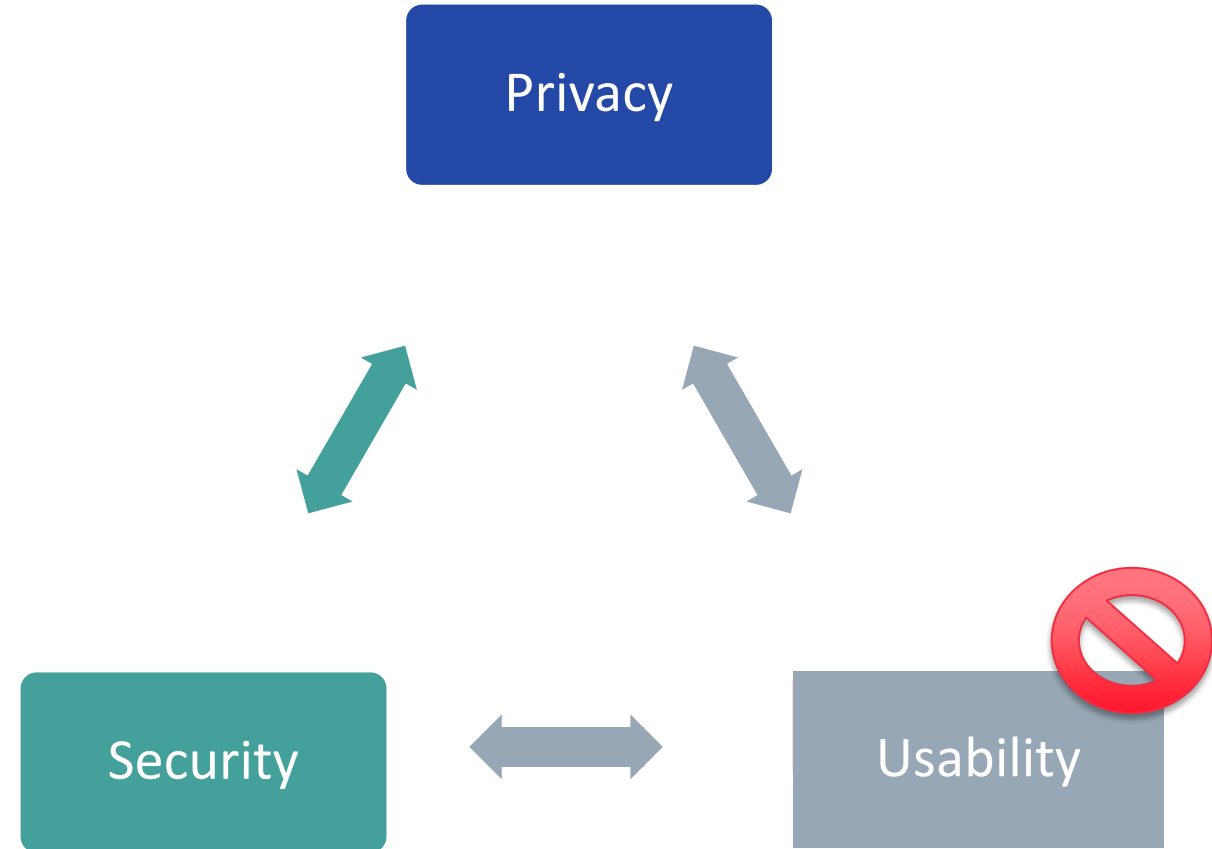


Deciding What to Apply



Don't Dismiss Usability

- Using the toughest controls in all scenarios may marginally improve posture
- ...but it will will also frustrate your customers and operations
- Agents are the closest to our customers of any staff



Use Force Only as Necessary

- Authentication assurance levels, step up authentication can be applied in customer service, too
- Lower-assurance challenges may be acceptable for lower-risk operations
- Higher-assurance challenges for higher-risk operations

Automate Thoughtfully

- Automating low-level requests reduces costs and risks of manual work
- Automating sensitive functions like account recovery could introduce new risks without additional controls
- Use automation and dynamic controls to augment processes that require human review

Key Takeaways - Customers

- Initial authentication procedures are critical
- Methods have been adapted to a limited communication channel; this creates trade-offs to weigh
- Different use cases may require a different bias for privacy, security, usability
- Layering methods for additional assurance at point of time is okay (step-up auth)

Your Workforce



Multi-Factor Authentication

- Always use MFA
- Users may not have access to USB ports or mobile phones
- OTP tokens are still common in physically constrained environments
- NFC, Bluetooth, etc. may occasionally be used

Authorization and Access

- Access control can be complicated by unique data sources and high degrees of change, ambiguity in work
- Data for automating access may require translation between multiple systems
- Customer service access requirements are often seasonal/fluid, challenging modern attribute-based access methods
- Overlapping job functions; separation of duties may be poor

More Complexity - Contractors

- Contractors may not use the same practices, technologies, standards for federation and identity management
- Consider technical interoperability as a requirement, not an implementation detail while selecting vendors

Key takeaways - Workforces

- Call center environments add complexity to selecting an MFA strategy
- Varied data sources, nonstandard job functions add complexity to access control systems and governance
- Reconciling external party requirements (such as contractors) on top of this adds further complexity and overhead; plan for this during vendor selection

Putting It All Together



Map the Current State



- Whether starting from scratch or managing change, you need to understand the ecosystem first
- Get to know your customer service stakeholders (agents, management)
- Learn what use cases, concerns, and KPIs/metrics they're accountable to (call handling time, customer satisfaction)
- Lean on **both** security and operations SMEs to build a threat model

Build a Risk Management Framework



Probability

Rare - 1

Unlikely - 2

Moderate - 3

Likely - 4

Almost Certain - 5

Impact

Minimal - 1

Low - 2

Medium - 3

High - 4

Severe - 5

Risk	Likelihood	Impact	Score	Control
PIN replay	2	5	10	Automated entry
Unauthorized purchase	3	4	12	SMS confirmation

...and prioritize, prioritize, prioritize.

Solutions May (or May Not) Be Technical

- Deploying new MFA hardware (non-technical, but operationally heavy), or supporting new authentication standards
- May also include workforce reorganization to limit access to sensitive privileges/data to smaller teams

Considerations for Change Management



- Customer service is downstream; change is difficult and not fully within their control
- Understand how changes impact the employees – vet solutions with your frontline staff
- When solutions cause churn and value isn't understood, people work around them

Applying What You've Learned

- Next week you should:
 - Meet with your customer service stakeholders, learn the structure of their business
- Within three months you should:
 - Document, threat model, and prioritize risk improvement areas
 - Define and vet solutions
- Within six months you should:
 - Define a roadmap to achieving the desired state for top 3-5 risks
 - Drive a project or program to implement solutions against those risks
 - Bring support personnel to your next conference 😊