



Cloud Without Borders; Global Security and Privacy

April 20, 2015, Cloud Security Alliance, San Francisco—Philippe Courtot from Qualys talked about global security and privacy as being an intertwined pair. Both are being threatened while users want more of each of them.

The two concepts are parallels to Doctors without Borders in that they are working in areas of greatest need. To prevent cyber diseases requires a complex set of actions: detect origins, intervene at the local level to be most effective, share information on the outbreak, setup quarantine protocols for entry and exit, develop vaccinations and delivery technologies, orchestrate the whole enterprise, and monitor disease and treatment progress.

Both security and privacy are becoming more public issues, and not just for the technical community. In the medical areas, disease severity has dropped over time, while in security to opposite seems to be occurring. The doctors tie immediacy and local infrastructure to global expertise and technologies. They develop best practices, standards, and certifications for all facets of the ongoing operations.

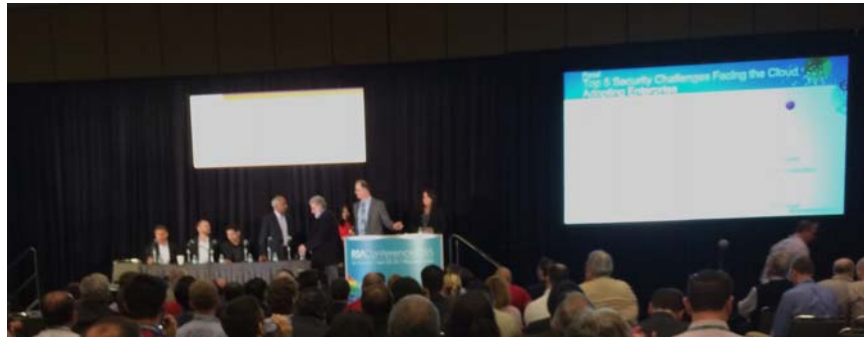
The same efforts are being attempted by the Cloud Security Alliance (CSA) to help all levels of users to become more data disease resistant. The CSA is improving its influence in many areas. For example, in Dubai the local agencies have adopted the CSA compliance and its monitoring capabilities as a part of their security dashboard.

Also like Doctors without Borders, the CSA has a flat organization, which helps improve agility. The organization depends on its staff and volunteers to do most of the work autonomously. The increasing levels of disruption are being developed and dispersed on a global scale, so the response has to rise to match the scale of the disrupters. As a result, security must change to mirror the technologies and capabilities of the criminals. First, the architectures and infrastructure must change to embed security as the starting point. Then all users and organizations have to change practices to increase collaboration and move from silos of defenses to a cloud platform that allows greater agility and intelligence within the security framework. Finally, the organization structures have to change to increase centralization and coordination of all the users.

Panel Discussion: “Top 5 Security Challenges Facing the Cloud Adopting Enterprise”

Sol Cates CSO, Vormetric
Jay Chaudhry CEO, Zscaler
John DiMaria ISO Product Manager, BSI

Rehan Jalil CEO, Elastica
Krishna Naraswamy Chief Data Scientist, Netskope
Chenxi Wang VP Cloud Security, CipherCloud



Copyright © 2015 Cloud Security Alliance

Major Themes @ RSAC

- Multi-Factor Authentication
- Cryptography
- Privacy
- Shadow IT
- IoT



Jim Routh CISO, Aetna



cloud
CSA security
alliance™

Shadow IT

- courtesy of Skyhigh Networks



cloud
CSA security
alliance™

Shadow IT

- courtesy of Skyhigh Networks

BUT MANY WOULD
BE SHOCKED
TO DISCOVER
THEY CONNECT TO
1,555
PARTNERS
VIA THESE APPS



CSA cloud security alliance™

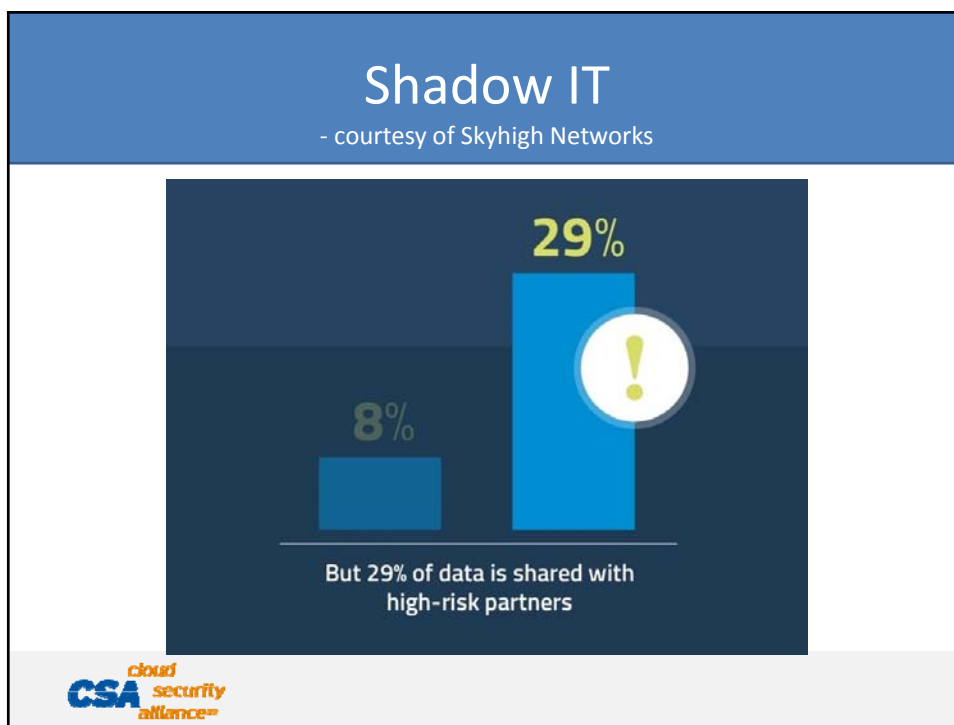
Shadow IT

- courtesy of Skyhigh Networks

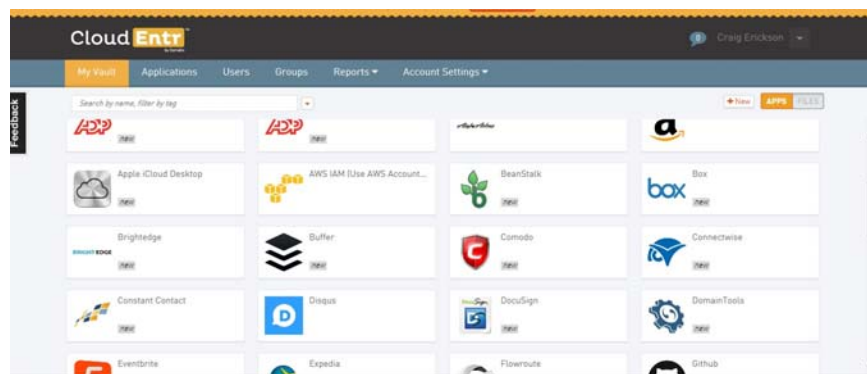
OUT OF THOUSANDS OF COMPANIES, A SELECT
58 "SUPER PARTNERS"
CONNECT WITH 50% OF ENTERPRISES



CSA cloud security alliance™



Governance of Shadow IT



Mobile Working Group
Peer Reviewed Document



Security Guidance for
Early Adopters of the
Internet of Things (IoT)

April 2015



Copyright © 2015 Cloud Security Alliance

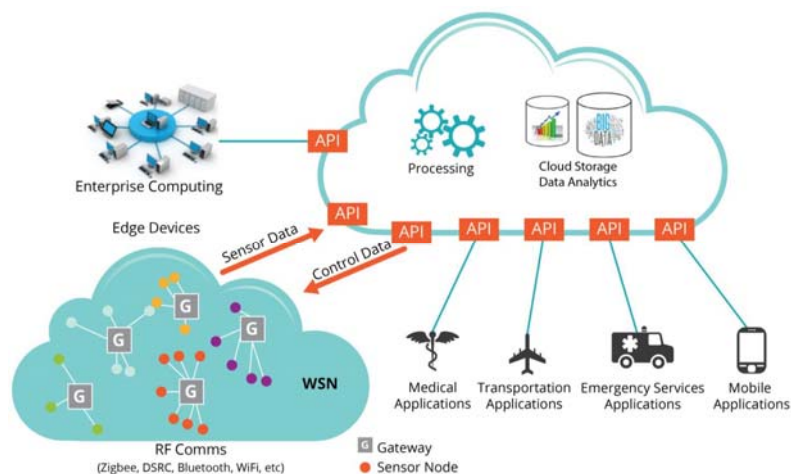
CSA Goals and Guideline Recommendations for early business adopters of the IoT

- Maintain confidentiality and integrity of business and personal data collected by provisioning of encryption, authentication and integrity protections throughout the IoT infrastructure
- Understand and address stakeholder privacy concerns prior to the implementation of the IoT capabilities by performing a privacy impact assessment
- Safeguard the infrastructure from attacks that target the IoT as a vector into an organization's assets, through the use of IoT device life cycle controls and a layered security approach
- Initiate a global approach to combat security threats by sharing threat information with security vendors, industry peers and CSA



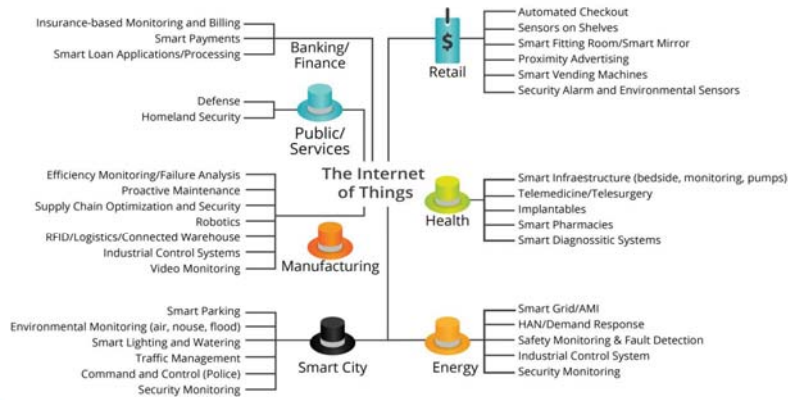
Copyright © 2015 Cloud Security Alliance

IoT & Cloud Computing



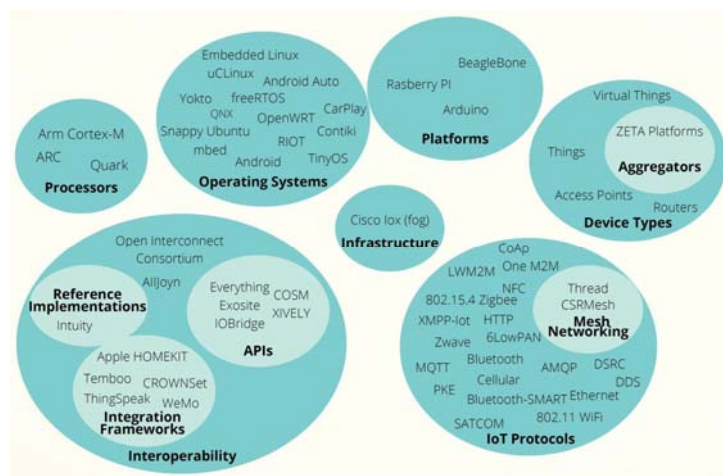
Copyright © 2015 Cloud Security Alliance

IoT Applications



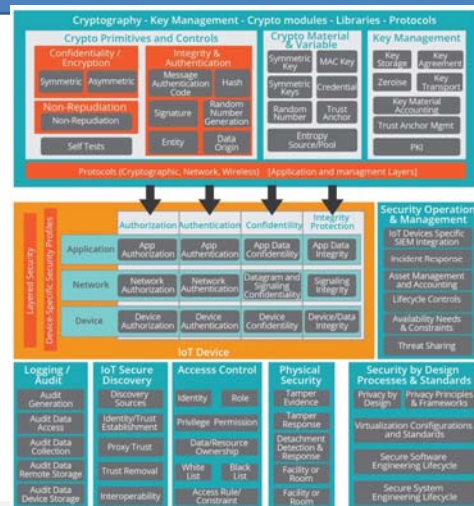
Copyright © 2015 Cloud Security Alliance

IoT EcoSystem



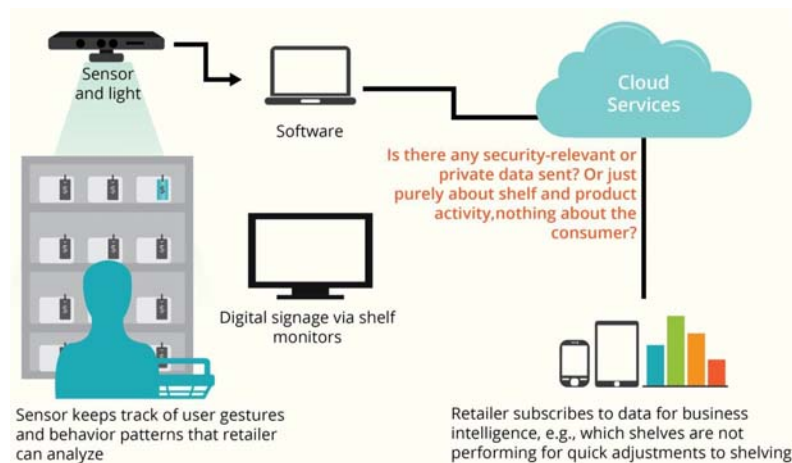
Copyright © 2015 Cloud Security Alliance

Recommended Security Controls



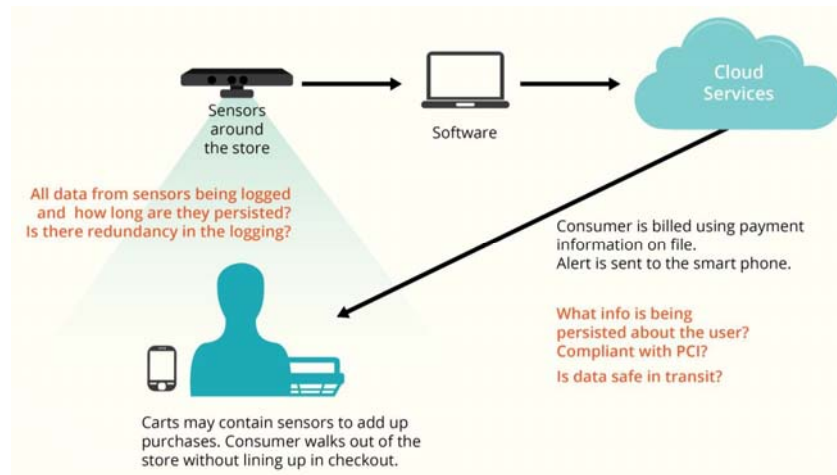
Copyright © 2015 Cloud Security Alliance

IoT Consumer Privacy Concerns



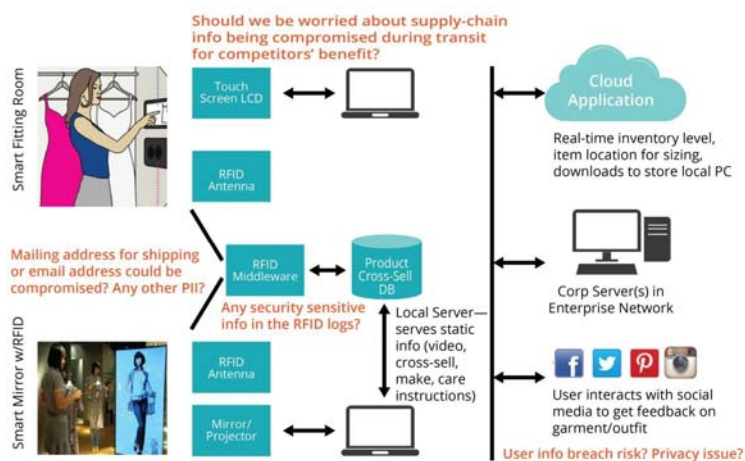
Copyright © 2015 Cloud Security Alliance

IoT Consumer Privacy Concerns



Copyright © 2015 Cloud Security Alliance

IoT Consumer Privacy Concerns



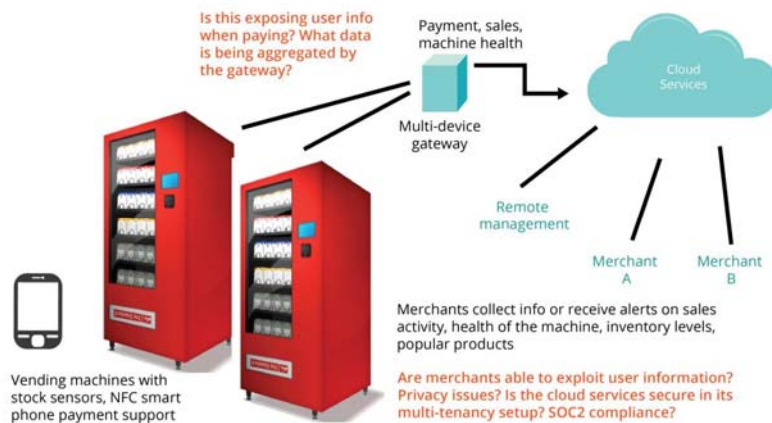
Copyright © 2015 Cloud Security Alliance

IoT Consumer Privacy Concerns



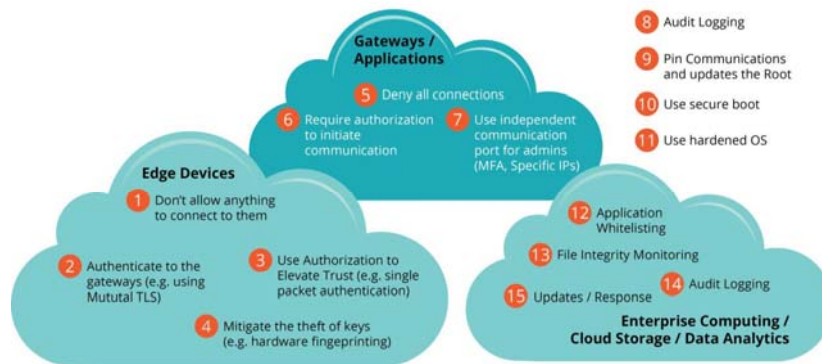
Copyright © 2015 Cloud Security Alliance

IoT Consumer Privacy Concerns



Copyright © 2015 Cloud Security Alliance

Elements of a Protection Architecture for IoT



Copyright © 2015 Cloud Security Alliance

How CSA's "Little Brother"



Implements CSA's IoT Guidance
Today



Copyright © 2015 Cloud Security Alliance

Copyright © 2015 FIDO Alliance



FIDO Privacy Principles

The design and implementation of FIDO Authenticators, Clients, and Servers must adhere to the following principles in order to be considered fully compliant. Just as we seek to protect the integrity of users' accounts, we also ensure that FIDO technologies are not used to identify users when they don't want or expect it.



Copyright © 2015 FIDO Alliance



FIDO Privacy Principles

#1 Require explicit, informed user consent for any operation using personal data

#2 Provide clear context to the user for any FIDO operations

#3 Limit collection of personal data to FIDO-related purposes

#4 Use personal data only for FIDO operations

#5 Prevent identification of a user outside of FIDO operations

#6 Biometric data must never leave the user's personal computing environment

#7 Protect FIDO-related data from unauthorized access or disclosure

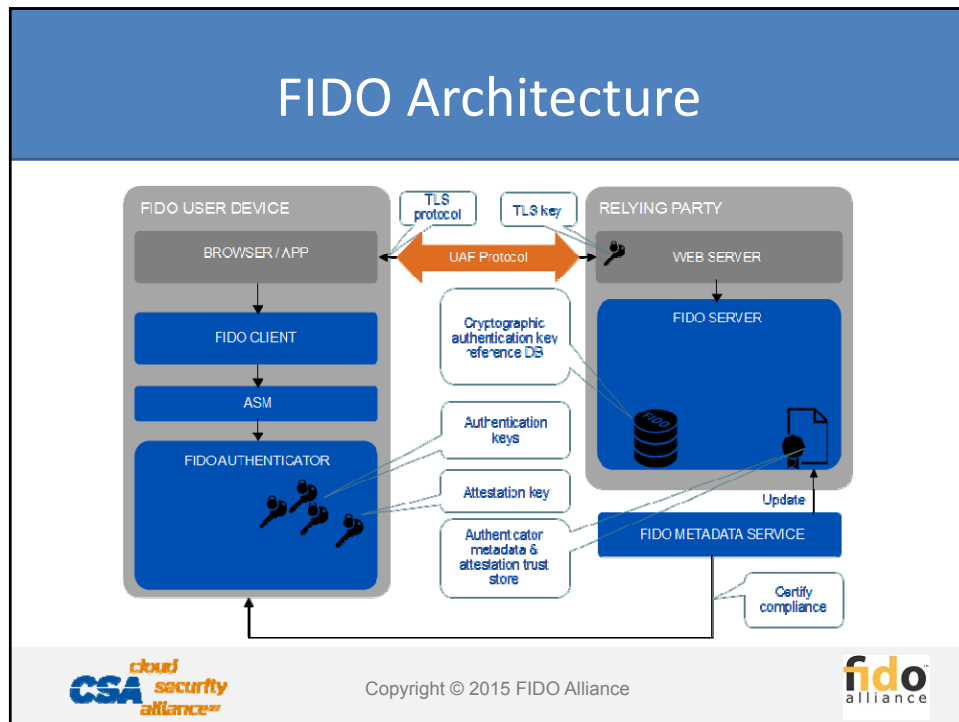
#8 Allow users to easily view and manage their FIDO Authenticators



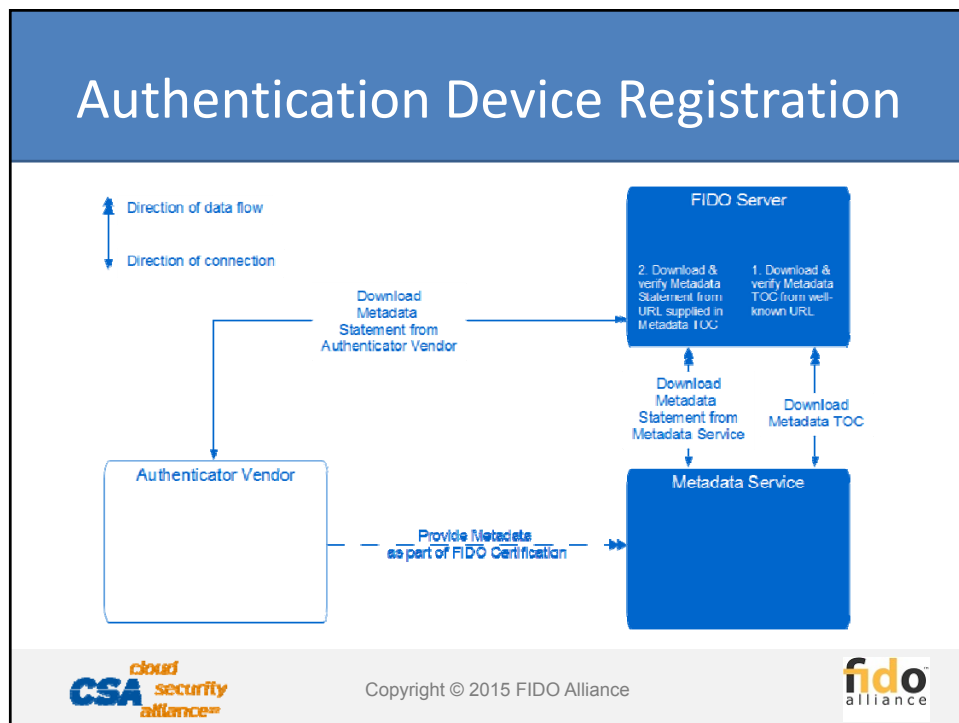
Copyright © 2015 FIDO Alliance



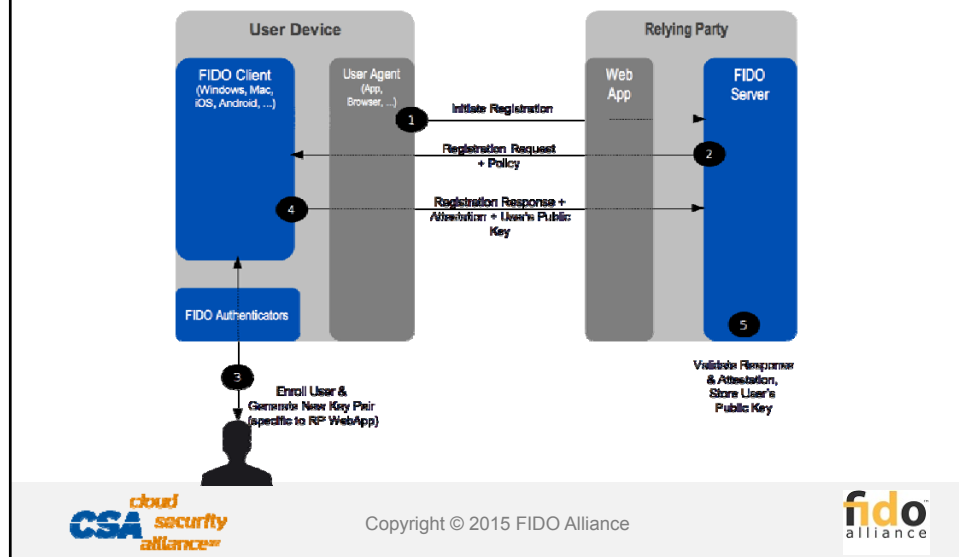
FIDO Architecture



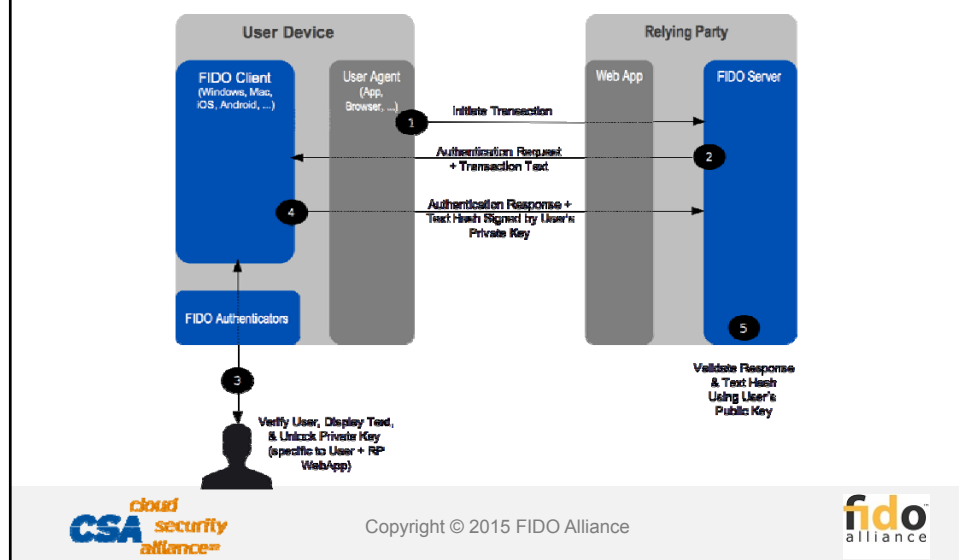
Authentication Device Registration



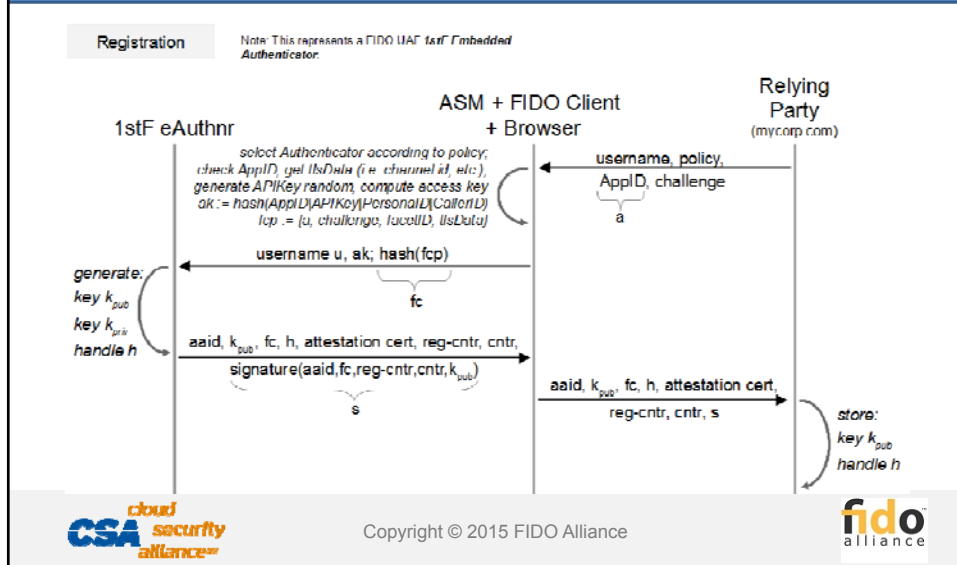
UAF Registration



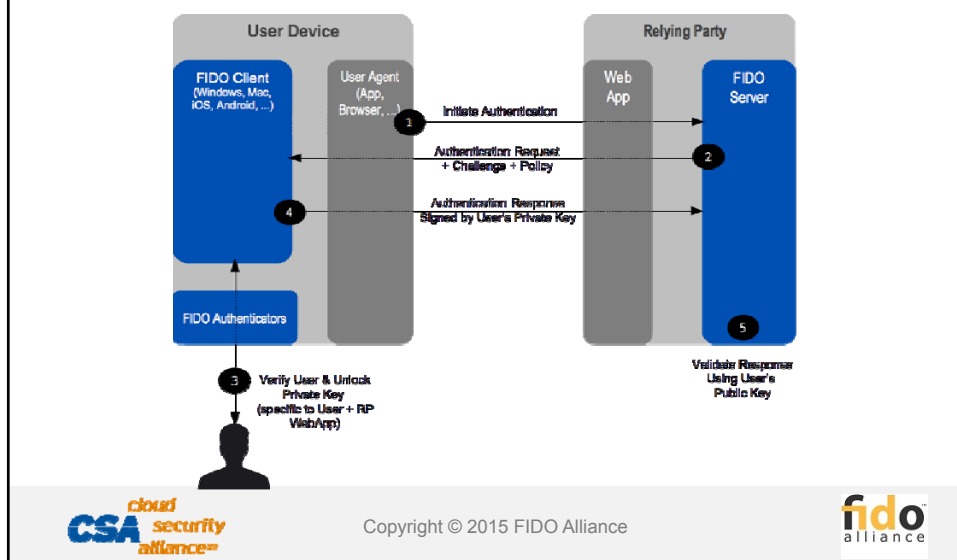
UAF Transaction



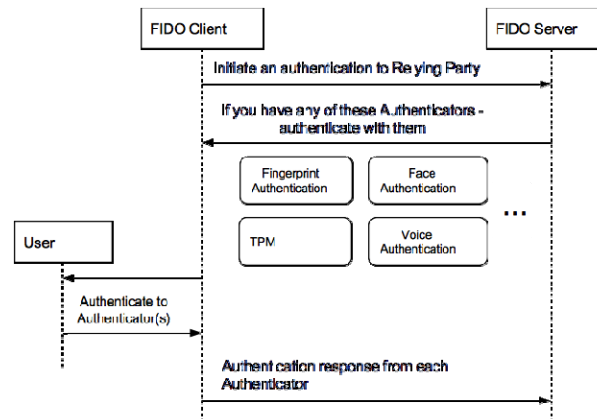
Authenticator Registration Technical Details



Authentication Process



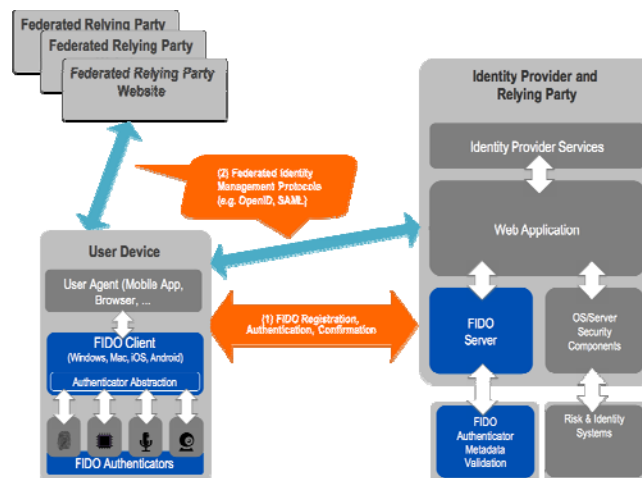
UAF Authentication Summary



Copyright © 2015 FIDO Alliance



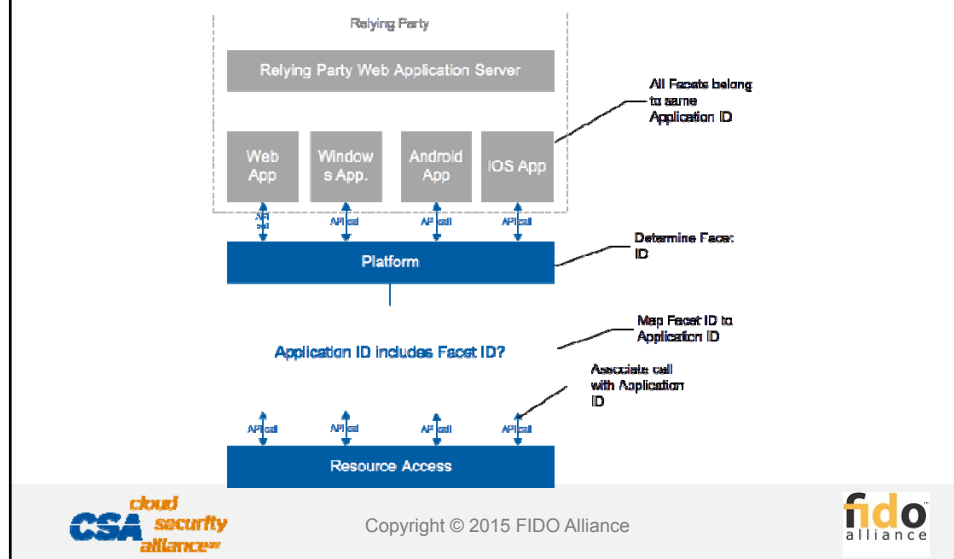
Federated Identity Implementation



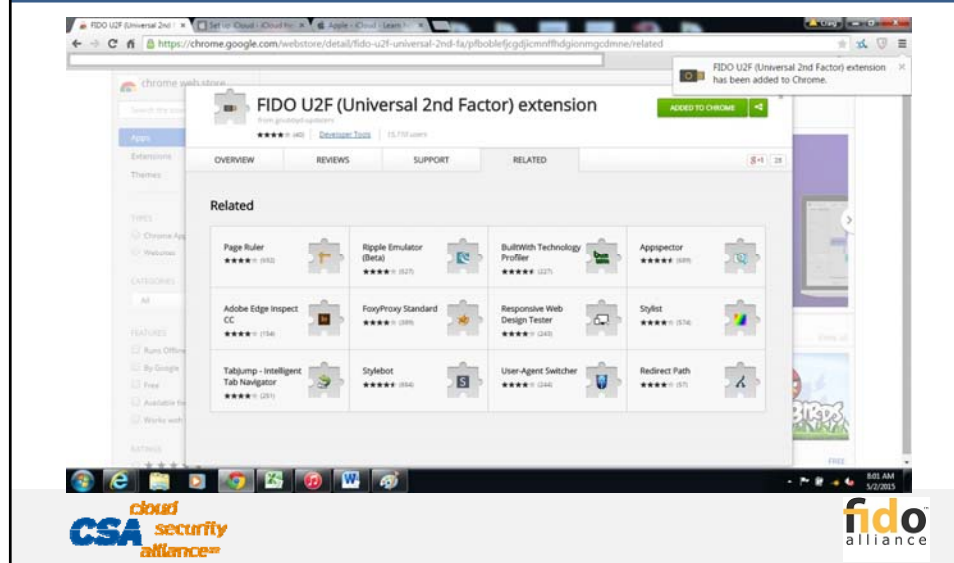
Copyright © 2015 FIDO Alliance



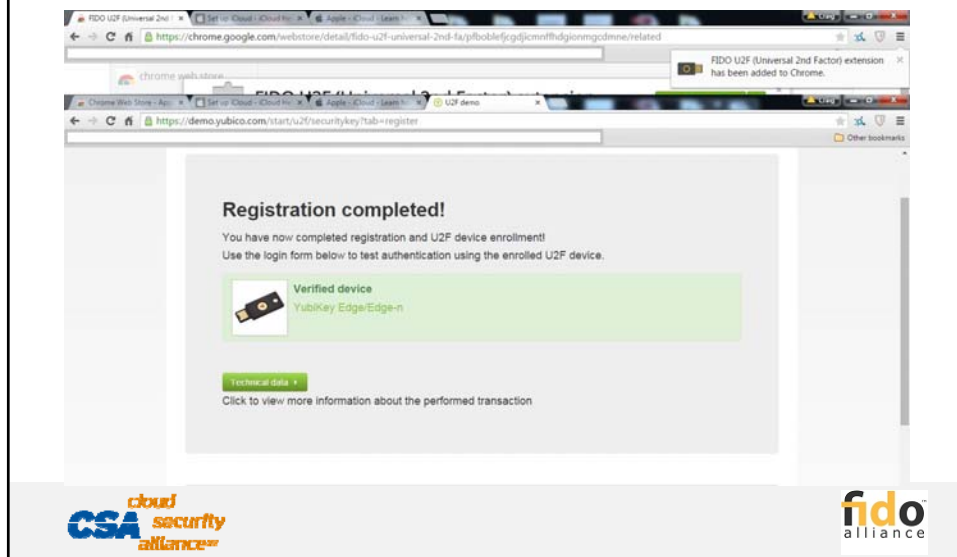
Multi-Device, Multi-Account Support for “Single Apps”



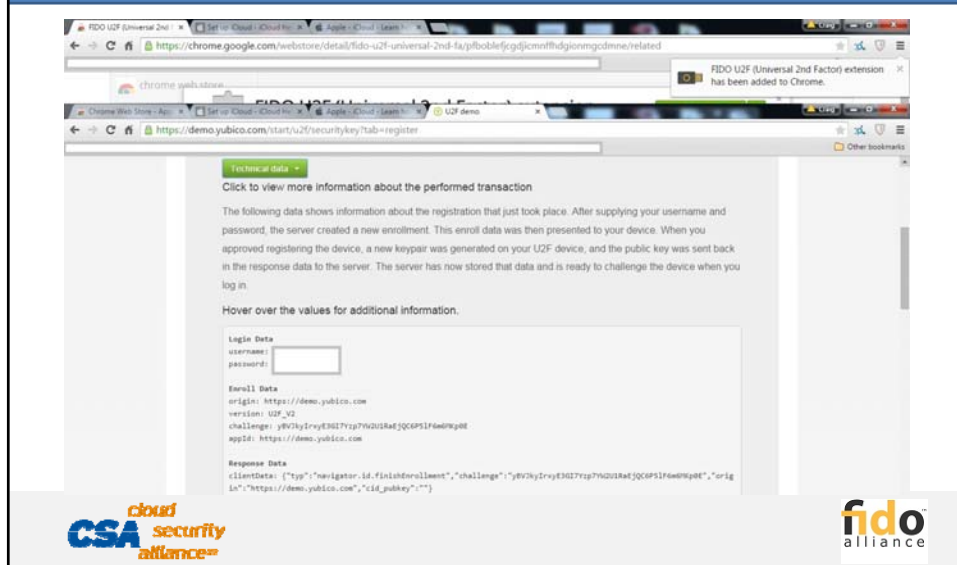
Apps Using the U2F Framework



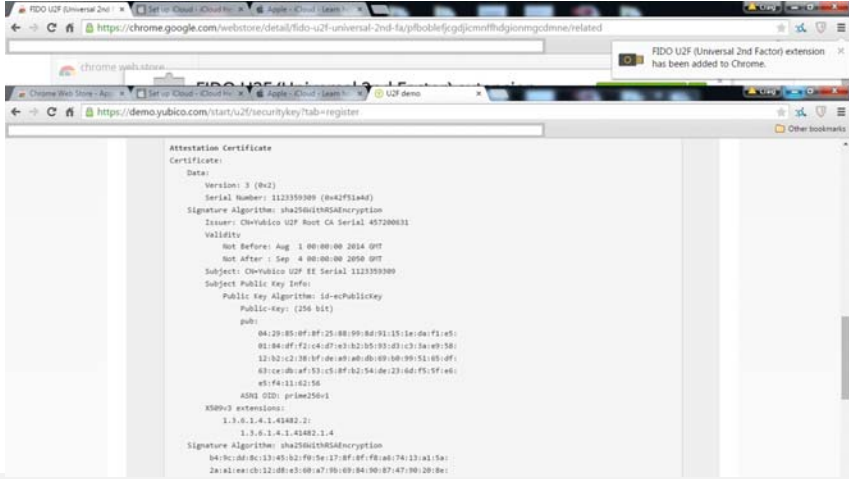
Registration for YubiKey



Registration Details



Registration Details

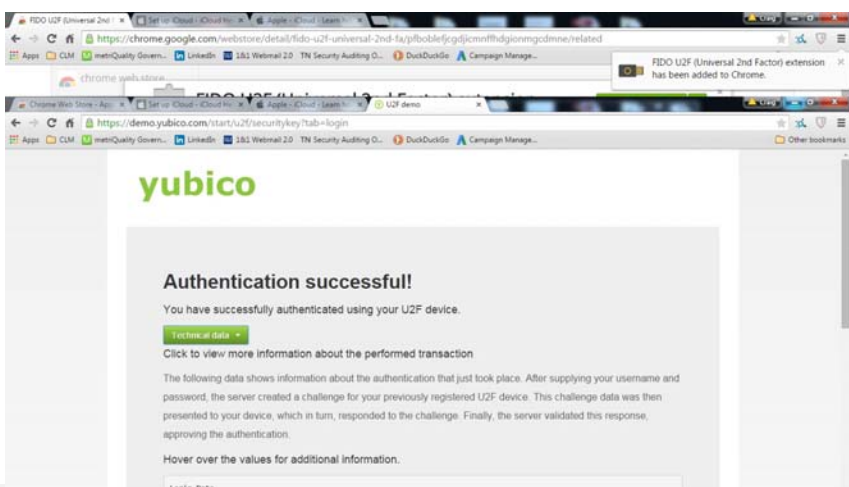


The screenshot shows a web browser displaying the Yubico U2F registration page. The URL is <https://demo.yubico.com/start/u2f/securitykey?tab=register>. The page displays an "Attestation Certificate" with the following details:

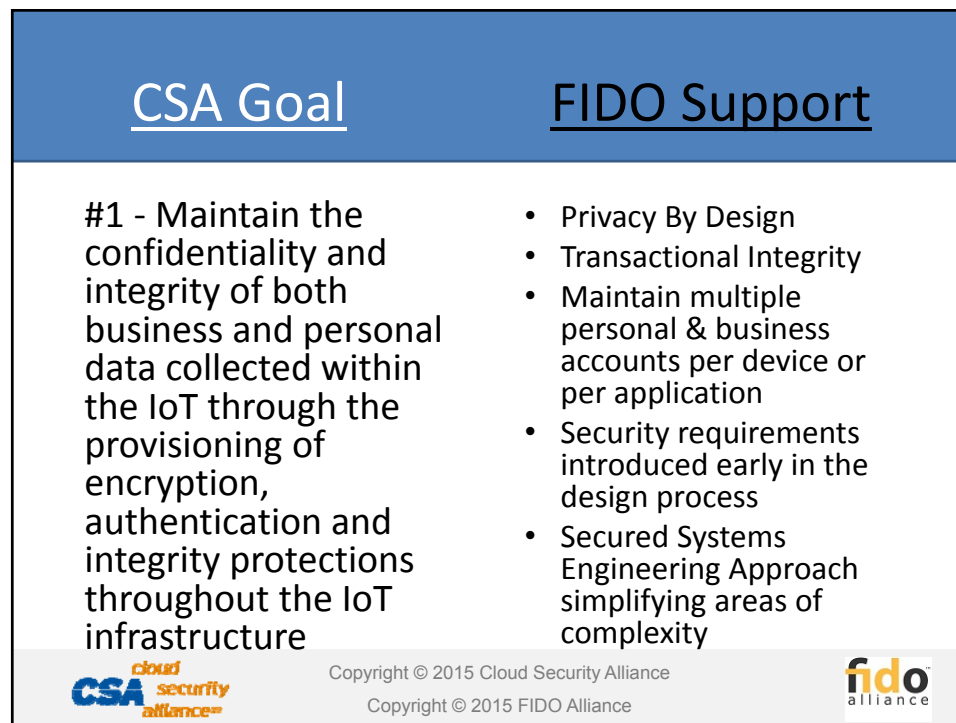
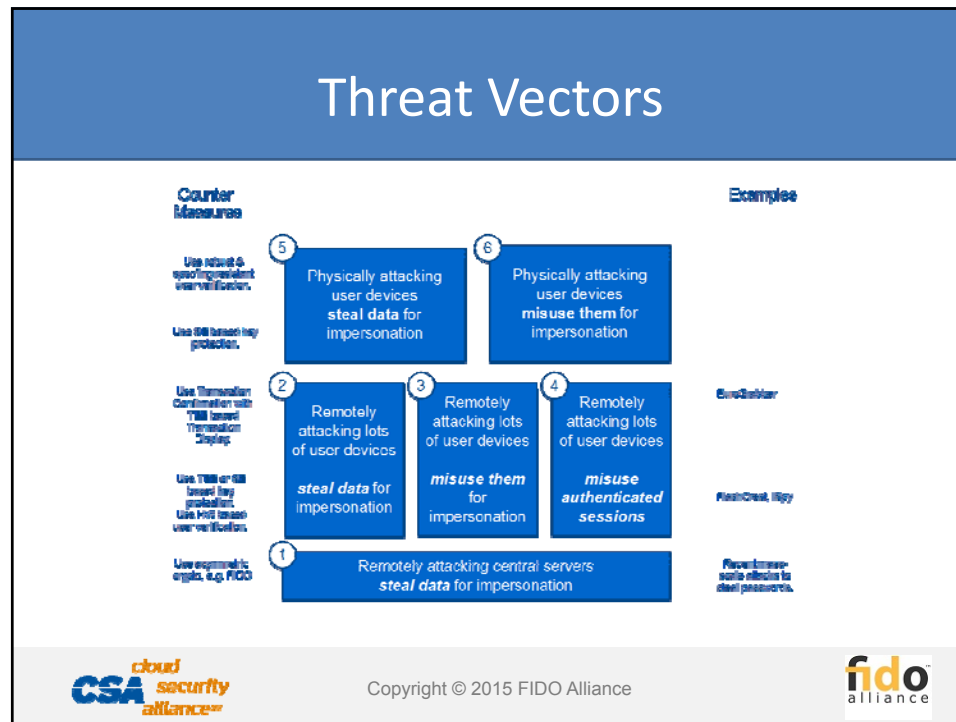
- Version: 3 (0x2)
- Serial Number: 1123359389 (0x42f51a4d)
- Signature Algorithm: sha256withRSAEncryption
- Issuer: ObVubico U2F Root CA Serial 457280631
- Validity:
 - Not Before: Aug 1 00:00:00 2014 GMT
 - Not After: Sep 4 00:00:00 2050 GMT
- Subject: ObVubico U2F EE Serial 1123359389
- Subject Public Key Info:
 - Public Key Algorithm: id-ePublicKey
 - Public key: (256 bit)
 - pub:
 - 04:29:85:0f:0f:25:00:09:8d:93:15:1e:da:f1:e5:
 - 01:04:df:f2:c4:0f:a3:b2:05:03:03:c1:3a:e9:5d:
 - 12:b2:c2:30:bf:de:a5:eb:db:09:00:09:51:65:0f:
 - 63:ce:ab:0f:53:c5:0f:b2:54:de:23:6d:f5:5f:ed:
 - e5:f4:33:62:56
 - ASN1 OID: prime256v1
- X509v3 extensions:
 - 1.3.6.1.4.1.4242.2:
 - 1.3.6.1.4.1.4242.1.4
- Signature Algorithm: sha256withRSAEncryption
- Signature:
 - 04:fc:0d:8c:13:4b:b2:fb:5e:17:0f:0f:fb:ad:74:13:a1:0a:
 - 2a:1a:ce:cb:12:0b:e3:00:a7:0b:00:04:50:87:47:00:20:de:

The page also features the CSA cloud security alliance logo and the FIDO alliance logo.

Authentication Using YubiKey



The screenshot shows a web browser displaying the Yubico U2F authentication success page. The URL is <https://demo.yubico.com/start/u2f/securitykey?tab=login>. The page displays a "yubico" logo and the message "Authentication successful!". Below the message, it states: "You have successfully authenticated using your U2F device." There is a link for "Technical data" and a link to "Click to view more information about the performed transaction". The page also includes a paragraph explaining the authentication process: "The following data shows information about the authentication that just took place. After supplying your username and password, the server created a challenge for your previously registered U2F device. This challenge data was then presented to your device, which in turn, responded to the challenge. Finally, the server validated this response, approving the authentication." and a note to "Hover over the values for additional information." The page also features the CSA cloud security alliance logo and the FIDO alliance logo.



FIDO Support for other CSA Guidelines

- Secure configuration using tamper-resistant enclosures, and mechanisms for tamper evidence and tamper response
- Encrypted Data-At-Rest on device contains no PII – only keys which cannot be linked to an individual or app
- Specific hardware / software versions of the devices' lifecycle can be managed
- Secure key management practices for creation, distribution and revocation, including standard processes for compromise recovery and initial registration



Copyright © 2015 Cloud Security Alliance
Copyright © 2015 FIDO Alliance



FIDO Mitigates Threats Addressed by CSA Guidelines

- Identity Spoofing
- Data tampering
- Repudiation – data can be traced to authenticated and authorized sources
- Standardized registration processes are well-defined and enforceable



Copyright © 2015 Cloud Security Alliance
Copyright © 2015 FIDO Alliance



