

Multi-Factor Authentication for SWIFT Alliance Access

Proven security, flexible deployment

Banks are continually targeted with sophisticated cyber attacks with the majority of breaches occurring due to compromised user credentials. With digital identities in hand, hackers can easily conduct fraudulent transactions with damaging consequences to customer trust, bank reputation and the bottom line. In response to these growing threats, SWIFT—the global provider of secure financial messaging services—has introduced a set of security controls which are mandatory for all SWIFT customers.

Rising to the Realities of Today's Cyber Threats

From organized crime groups to state sponsored attacks, banking fraud is growing at alarming rates. Persistent, adaptive sophisticated attacks have plagued a number of banks across the globe. Over the past year, criminals used methods to compromise weak security in local networks accessing the banks' systems and initiating fraudulent SWIFT payment instructions worth well over hundreds of millions of dollars.

In the cyberattacks on banks in Bangladesh, Vietnam, the Philippines and Ecuador, the criminals followed the same basic pattern:

- 1 Attackers used malware to circumvent a bank's local security systems.
- 2 They gained access to the SWIFT messaging network.
- 3 Fraudulent messages were sent via SWIFT to initiate cash transfers from accounts at larger banks.

+1-888-690-2424

entrustdatacard.com
SecureSWIFT

 **@EntrustDatacard**

 **+entrust**

 **/EntrustVideo**

 **/EntrustSecurity**

Solution Benefits

- Deploy fast – deploy your way with cloud, turnkey appliance or traditional software
- Proven security helping the world's leading banks address fraud and compliance
- Build at your pace – start with simple use cases and expand as your business evolves
- Unmatched range of authenticators to meet cost, security and UX
- Native adaptive authentication improves security / ease of use
- Deploy OTP or PKI or both to meet your diverse needs
- Future proofed with optional device reputation, fraud detection and transaction signing modules

For more information on
Entrust Datacard Authentication please visit:
▶ entrustdatacard.com/SecureSWIFT



Multi-Factor Authentication for SWIFT Alliance Access

Proven security, flexible deployment

Banks Urged to Tighten Security as Hacks Continue

In response to these attacks, SWIFT has introduced a set of mandatory security controls and standards whereby customers are expected to comply to safeguard their systems against cyber heists. Applying these standards will raise the security bar for banks on the SWIFT network and further support customers in their efforts to prevent and detect fraudulent use of their infrastructure.

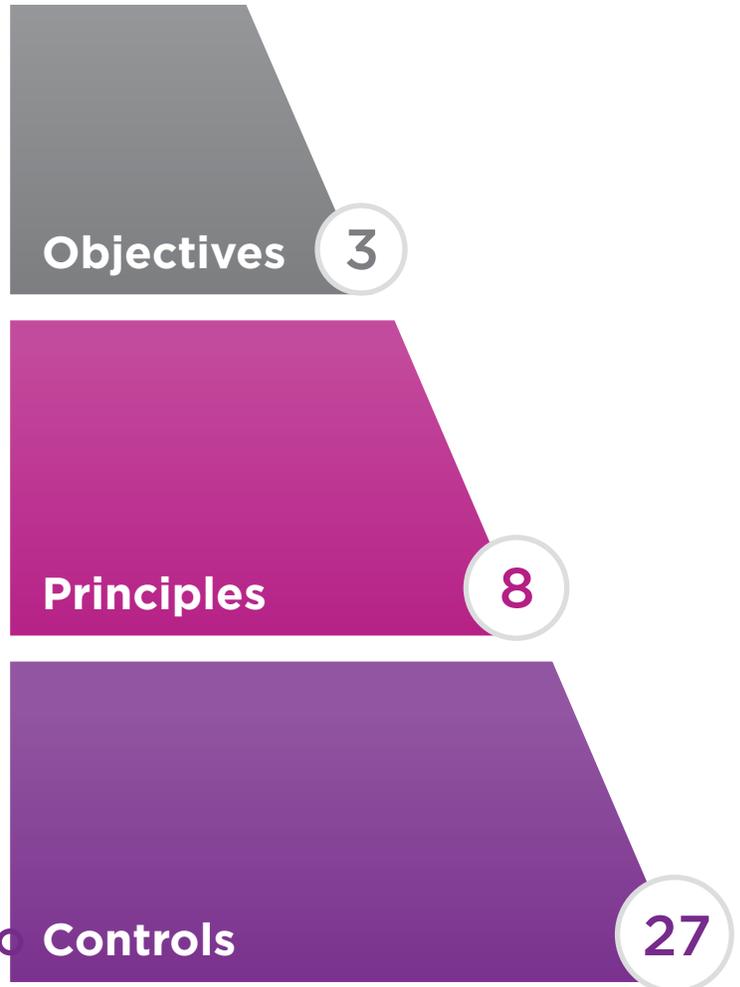
SWIFT greatly emphasizes the Prevention of Compromised Credentials or Identity Theft as part of the CSP Security Control Framework – Point no. 5. Usage of Strong Multi-Factor Authentication (and Password Policies) for interactive user access to SWIFT-related applications and operating system accounts is to be adopted by all partner banks and financial institutions.

SECURITY CONTROLS

CSP Security Controls Framework

Secure Your Environment	1	Restrict Internet access
	2	Segregate critical systems from general IT environment
	3	Reduce attack surface and vulnerabilities
	4	Physically secure the environment
Know and Limit Access	5	Prevent compromise of credentials
	6	Manage identities and segregate privileges
Detect and Respond	7	Detect anomalous activity to system or transaction records
	8	Plan for incident response and information sharing

Formal publication of Security Controls Framework on www.SWIFT.com in April 2017



Controls

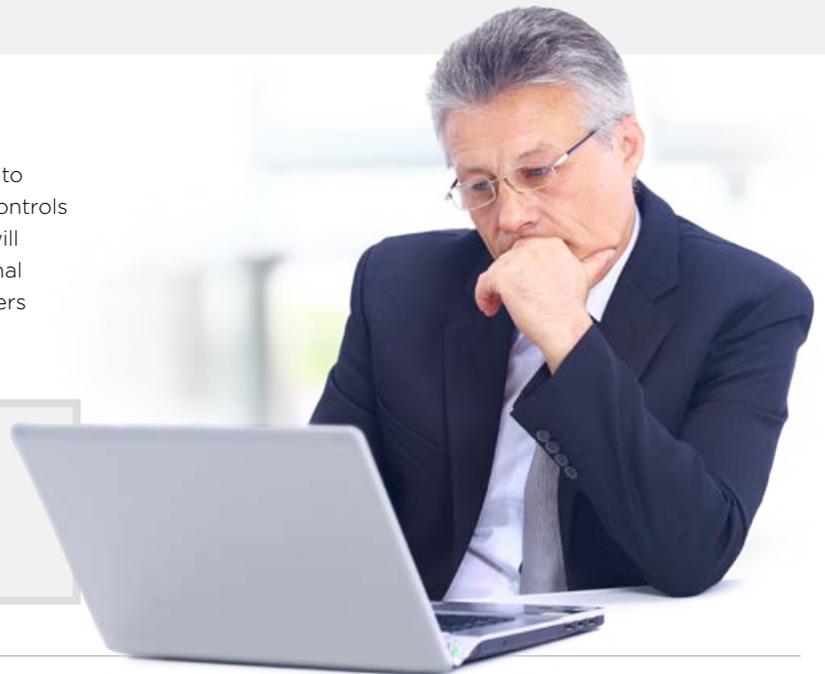
27

Deadlines Approaching

To ensure adoption, SWIFT will start requiring customers to provide detailed self-attestation against the mandatory controls from Q2 2017. Enforcement of mandatory requirements will start from January 2018, including inspections from internal and external auditors conducted with samples of customers to check quality.

More Details

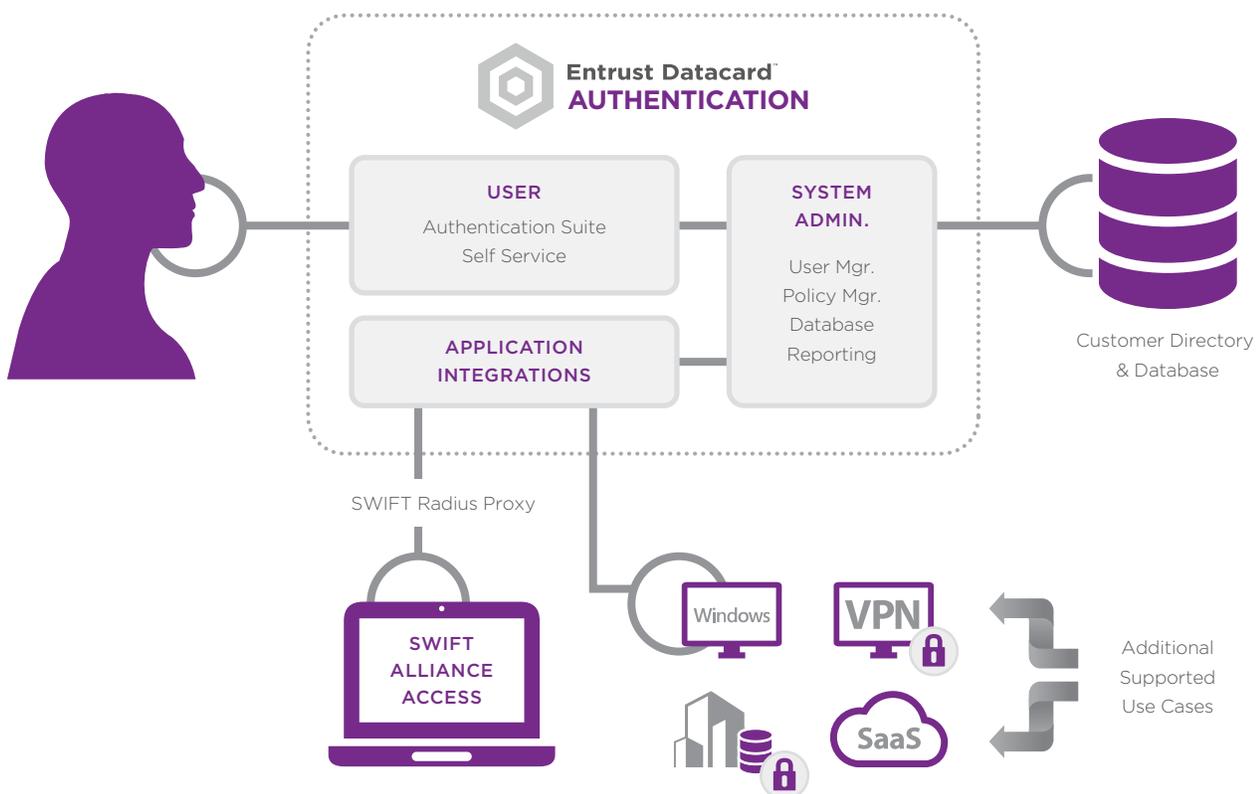
► <https://www.swift.com/myswift/customer-security-programme-csp/security-controls>



Compliance Made Easy — And Without Compromise

Entrust Datacard can help you address SWIFT compliance with trusted identity and secure transaction solutions adopted by banks across the globe. Our turnkey integration to the SWIFT Alliance Application means you deploy addressing compliance and stop fraud in its tracks.

With Entrust Datacard, we provide the flexibility to deploy multi-factor authentication quickly and easily in the most critical areas of your business—and then, as your needs grow, our solutions will be there to meet your evolving needs.



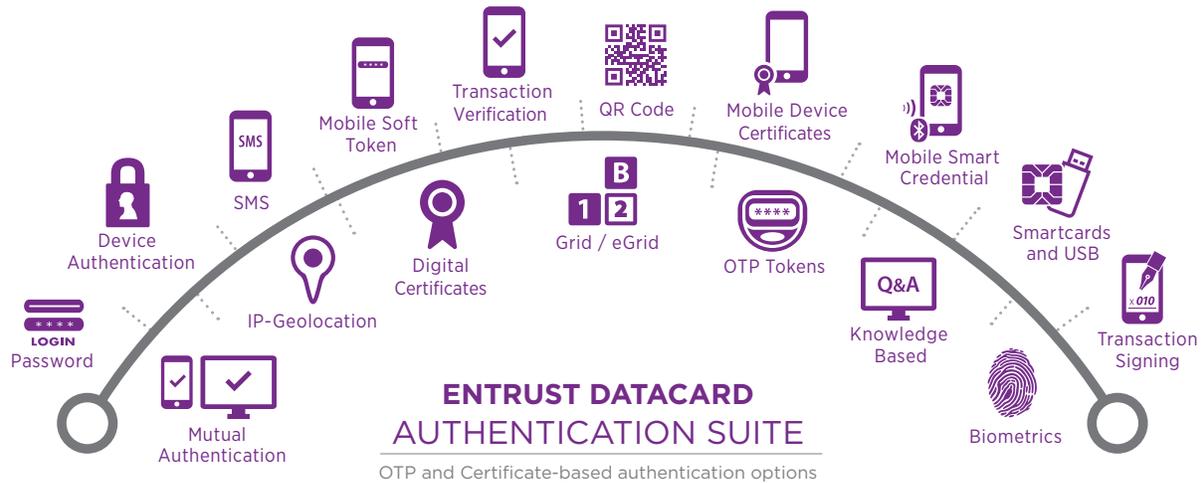
Multi-Factor Authentication for SWIFT Alliance Access

Proven security, flexible deployment

One Platform—Broad Suite of Authenticators—Native Adaptive Policies

Entrust Datacard provides more than a simple one-step means of protecting the world's largest and most respected banks and financial institutions (FI). The flexibility of our platform allows specific authenticators to be defined on a per-application and/or group basis, so you can tailor security to each use case or risk situation. Simple policy change can seamlessly adjust the authentication behavior of all applications almost instantly, without having to re-architect applications. This agility allows you to proactively protect what matters most.

Virtually all of our authenticators — from mobile and OTP tokens to transaction signing and grid cards — can be customized to feature your brand and native adaptive techniques help minimize user friction while augmenting security. Entrust Datacard offers a number of key features that are critical to any digital banking strategy helping you secure all your needs including employee, customer and partner access to your banking services.



Flexible Deployment Options



The choice is yours. Get up and running in minutes with our cloud service, deploy our turnkey virtual appliance in hours or build your own environment leveraging our enterprise software version.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email entrust@entrust.com or visit www.entrust.com.

Stronger Security - Better User Experiences

As market forces continually change, you need to be prepared with new lines of defense and more streamlined access methods for users. Entrust Datacard provides a broad suite of identity-based capabilities that can be deployed when the time is right for you. The solution includes:

- Device Reputation
- Transaction Verification
- Digital Signatures
- Real-time Fraud Detection

Headquarters

Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

