A SECURE TECHNOLOGY ALLIANCE IoT SECURITY COUNCIL AND PAYMENTS COUNCIL WHITE PAPER

IoT and Payments: Current Market Landscape

Version 1.0

November 2017

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Copyright © 2017 Secure Technology Alliance. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Secure Technology Alliance. The Secure Technology Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1 Introduction

The Internet of Things (IoT) is growing rapidly—8.4 billion connected "things" are forecast to be in use in 2017. That number is expected to increase to 20.4 billion in 2020,[1] and starting in 2017, the IoT market is projected to be worth more than $1 billion annually.[2] "Things" range from thermostats to automobiles, are used by individuals and businesses, and enable use cases that only a few years ago seemed like fiction. Cars talk to each other, and your refrigerator can order groceries.

One major use case that is expanding to the IoT is payment. Payment is now possible using a phone, wearable, or home assistant and is spreading to virtual or augmented reality experiences and connected cars. However, as the number of connected things increases, the number of end points vulnerable to attack also increases. Recent high profile IoT attacks (such as the malware attack using Mirai[3]) illustrate the vulnerability of certain IoT devices. While consumers demand the ability to make a payment wherever they are and with whatever device they are using, they also want the transaction to be frictionless and secure. This demand creates a challenge for merchants, issuers, and acquirers.

This white paper was developed by the Secure Technology Alliance to provide an overview of the current landscape for IoT payments. The paper discusses major environments and use cases for IoT payments, security threats to IoT payments, and considerations for implementing payments with IoT devices. The white paper focuses primarily on IoT device payments made using the traditional payment infrastructure (i.e., credit and debit). However, IoT payments are expected to expand beyond the traditional payment infrastructure, with additional discussion of the future of IoT planned for future projects.

[1] Gartner Newsroom press release, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," Feb. 7, 2012, http://www.gartner.com/newsroom/id/3598917.

[2] Statista, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[3] Wired, "The Botnet that Broke the Internet Isn't Going Away," Dec. 9, 2016, https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

2 What Are IoT Payments?

The story of the Internet of Things (IoT) has two parts: the evolution of devices that are now connected to the Internet, and the movement towards the machine-to-machine economy in which newly connected devices interact with each other.

Connecting more devices opens the door to developing new digital experiences for both consumers and businesses. One such experience is the payment transaction, including both the ability to pay and the ability to accept payment.

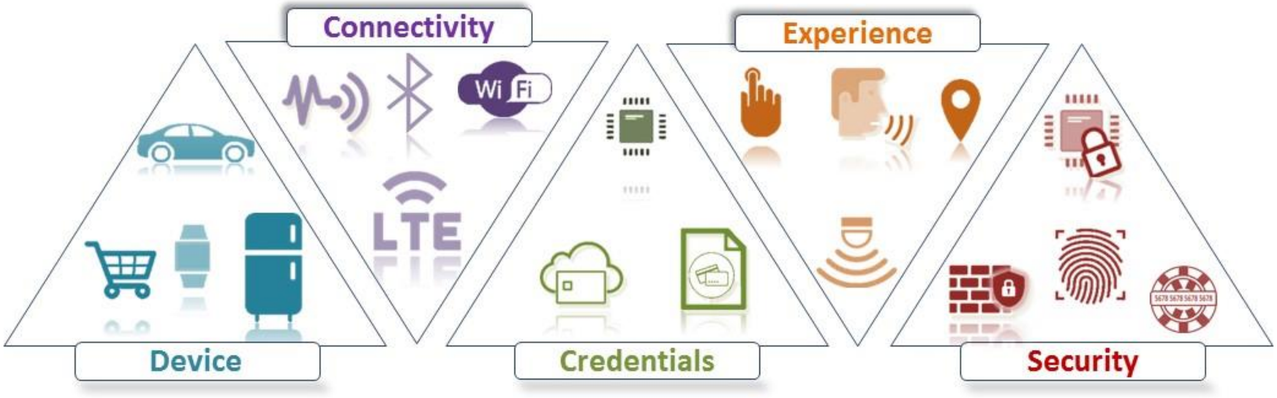
Digital payments continue to evolve, with the inclusion of payment-enabled IoT devices augmenting the browser and mobile payment experience. Consumers can pay using a range of newly connected devices, including connected cars, household appliances, and most recently, wearables. In parallel, the IoT is also changing the retail point of sale to include a number of new touch points, including parking meters, fitting room mirrors, and vending machines.

As a result, financial institutions, payment providers, and technology companies can now create innovative capabilities that deliver increasingly frictionless, relevant, and secure payment experiences.

Figure 1 illustrates the five key aspects of IoT payment:

- Device
- Connectivity
- Credentials
- Experience
- Security

Figure 1. Key Aspects of IoT Payments Implementations



As shown in Figure 1**,** IoT devices range from small wearable devices and shopping carts to home appliances and cars. The IoT device uses a connectivity channel to trigger a payment transaction, with technology depending on the environment. Payment credentials can be stored remotely in the cloud, or locally, in a secure element, depending on the form factor and payment use case. The consumer experience can vary; it ranges from pushing a button or using voice commands to a frictionless experience based on location or sensors. Data is secured using a variety of techniques to authenticate the consumer and transmit the payment credentials securely.

3 Major IoT Environments Implementing Payments

IoT payments can be implemented in a variety of environments, including:

- Automotive
- Homes
- Wearables
- Industrial
- Retail

3.1 Automotive

Today's intelligent and connected cars include a wide range of convenient features for consumers, from emergency services, smart driving assistance, and predictive maintenance to comfort and infotainment. By leveraging secure vehicle connectivity and technologies such as geo-location and voice-activated controls, a connected car can act as payment form factor. Payment functionality can provide drivers with seamless transactions to pay for a variety of goods and services, including parking, gas, tolls and food at drive-through restaurants.

3.2 Homes

Smart homes are one of the fastest growing IoT verticals, due to their potential to meet consumer demands for automation, sustainable living, efficient energy consumption, safety, security, and convenience. Smart home devices usually include the following:

- Data capturing capabilities, through sensors or other means
- Built-in or cloud-based processing intelligence
- Internet connectivity (directly through a mobile network or the home's network, such as WiFi, or through another device, using Bluetooth)

Connected smart home devices range from thermostats to appliances. They can be provisioned with or linked to payment credentials that can be used to pay for products or services.

3.3 Wearables

Wearables include more than just a trendy wristband or a fancy pair of headphones. Smart watches and wristbands are the dominant wearables form factors, although other form factors, such as rings, necklaces, glasses, shirts, shoes, virtual reality headsets, lenses, and smart tattoos, are becoming common.

Wearables can enhance various use cases, given their ability to process information with smart sensors and chips while connected to the Internet. A wearable can be active or passive. An active wearable has its own battery and connectivity to the Internet. A passive wearable receives power and connectivity from an external paired device.

As the contactless payment infrastructure expands and matures at the point of sale, wearables are a perfect form factor for payment. Wearables can host an embedded secure chip or have the capability for secure software emulation (such as using host card emulation (HCE) or a Trusted Execution Environment (TEE)), and can perform a secure payment transaction. Wearables are of great interest to issuers, who want to eliminate the use of cash for small purchases.

3.4 Industrial

Industrial digitization is a global trend. Digitization provides insights into production and reduces costs by optimizing machine performance. As the connectivity of machines increases, secure platforms are increasingly common, to ensure secure communication, facilitate software patches, and provide performance insights.

Industrial digitization is moving from a reactive service model to a proactive service model. Remote access relying on fragmented information is being transformed into proactive monitoring to avoid unnecessary service costs and predict maintenance scheduling. Further use cases include configuration, integration, and warranty management. Different smart pay-per-use models and billing models are opening the door for industrial equipment to include payment capability.

3.5 Retail

Consumers are always looking for highly personalized service on demand, pushing merchants to adopt new technologies to provide such service.

The retail industry is using IoT technologies to help optimize the supply chain, using smart shelves to track stock levels to trigger replenishment and monitor the goods validity. Smart price tags generate new revenue streams by altering pricing based on demand and market trends.

Merchants are leveraging connectivity to customer devices to upsell related products and enable consumers to browse available inventory, consult reviews and market trends, and obtain service plans. Secure connectivity allows merchants to offer customers frictionless checkout, using technologies such as geo-location services and contactless or in-app payments. This connectivity also enables merchants to expand the point of sale to include in-store surfaces such as mirrors and storefront windows, with payment either taking place in an app or through contactless payment capabilities embedded in the devices.

4 Use Cases and Pilots for IoT and Payments

Several IoT payment use cases have been proposed. Some have been facilitated by the payment networks (e.g., Mastercard, Visa) and some by technology enablers (e.g., Samsung, IBM). This section describes some of the more prominent use cases and pilots.

4.1 Payments Using Smart Home Electronics

It is now possible to make payments using a refrigerator or a smart home assistant such as Amazon Echo or Google Home.

4.1.1 Refrigerator Grocery Shopping

Groceries™ by Mastercard is an app that enables consumers to order groceries using Samsung's Family Hub refrigerator.[4] Household members can build, manage, modify, and share grocery lists and shopping carts and purchase the groceries from nearby grocery stores. The final shopping list must be approved with a 4-digit PIN. Items are then paid for in a simple, single-checkout experience that accepts any U.S.-issued credit or debit card.

When launched, the app connects to FreshDirect or ShopRite. Although the app was developed by Mastercard, consumers can link the app to any U.S.-issued credit or debit card.

4.1.2 Smart Home Assistants

Both major home assistant products, Amazon Echo and Google Home, support voice ordering, as do several other home assistants. To order using Amazon Echo, the desired payment method must be set up in an Amazon account. Unauthorized ordering can be avoided by requiring use of a 4-digit PIN. To order using Google, the payment method must be set up using Google Home.

4.2 Payments Using Wearable Devices

The wearable devices most commonly used for payments are smart watches. The Samsung Gear S3, Apple Watch, and LG Watch Sport, all widely used smart wearable devices, also include payments capability. Most wearable payments use cases support in-store contactless payments, and some wearable devices also support in-app payments. Some smart watches, such as the Apple Watch, provide a true IoT payment experience, allowing the consumer to use the browser on a Mac to shop and then check out using the Apple Watch as a form of authentication (by double clicking the side button) to complete the payments process.[5]

Another potential wearable use case involves shoes. IBM and Visa announced a partnership[6] in February 2017 to bring the secure IoT commerce and payment experience to consumers. One use case promoted by the announcement was that a running shoe that is about to wear out could alert the runner and help the runner purchase a replacement pair.

[4] Mastercard, "MasterCard, Samsung Make Everyday Shopping Easier in Tomorrow's Smart Home with Launch of Groceries by MasterCard App," press release, Jan. 5, 2016, https://newsroom.mastercard.com/press-releases/mastercard-samsung-make-everyday-shopping-easier-in-tomorrows-smart-home-with-launch-of-groceries-by-mastercard-app/,

[5] Apple, "Safari for Mac: Shop with Apple Pay in Safari," https://support.apple.com/kb/PH25811?locale=en_US.

[6] IBM, Internet of things blog, https://www.ibm.com/blogs/internet-of-things/visa/.

A third wearables use case involves fitness trackers. Mastercard announced its entry into the fitness tracker space on August 2017, enabling Fitbit's first smartwatch, Fitbit® Ionic™, and Garmin's vivoactive® 3 device to make secure, tokenized contactless payments.[7] Starting in late 2017, health and fitness enthusiasts will be able to make contactless payments at millions of merchant locations globally, freeing active users from having to carry their wallets or smartphones.

4.3 Payments in Virtual or Augmented Reality

Both virtual reality (VR) and augmented reality (AR) provide immersive experiences, a concept that retailers can leverage to enhance the shopping experience. VR can closely emulate in-store shopping, and AR can enhance the shopping experience for a consumer who is in a store.

Mastercard has already demonstrated that shopping and payment can be integrated into a VR experience. [8] The simple use case allows a consumer playing a round of virtual golf to look at the golfer's shoes (or other apparel); a pop up window then displays the make, manufacturer, and available sizes and colors. The consumer can choose an item to purchase and check out using Masterpass.

4.4 Connected Car Payments

A connected car offers the potential for multiple interesting use cases. Some of the proposed use cases include making service appointments, ordering replacement parts (such as belts or oil), refueling, parking at smart parking locations, and ordering at a drive-through window. Payment is central to all of these experiences. The payments can be remote, card-on-file payments or can leverage other means (e.g., NFC, Bluetooth Low Energy (BLE), QR codes) to exchange a secure payment token between the car and the merchant.[9]

In October 2016, Mastercard announced that it was working with General Motors (GM) to develop the OnStar Go platform, a new cognitive mobility platform that enables drivers to pay for transactions such as picking up food at a drive-through window or filling the gas tank from the comfort of their GM vehicle.[10] Initial rollout leverages Mastercard's payment gateway with stored tokenized credentials. Online customers will be able to pay for OnStar satellite services, as well as parts and accessories, through the more than 4,000 Chevrolet, Buick, GMC, and Cadillac dealerships in the United States.[11]

[7] Mastercard, "Mastercard Makes Post-Workout Shopping A Breeze For Fitbit Users," press release, Aug. 28, 2017, https://newsroom.mastercard.com/press-releases/mastercard-makes-post-workout-shopping-a-breeze-for-fitbit-users/.

[8] Mastercard, "Masterpass AR/VR: A unity project for quickly integrating Masterpass into your augmented or virtual reality experience," https://developer.mastercard.com/product/masterpass-ar-vr.

[9] Visa, "Let your car pick up the tab," https://usa.visa.com/visa-everywhere/innovation/let-your-car-pick-up-the-tab.html.

[10] Mastercard, "Mastercard Joins Onstar Go, the Auto Industry's First Cognitive Mobility Platform Delivered by IBM and General Motors," press release, Oct. 26, 2016, https://newsroom.mastercard.com/2016/10/25/mastercard-joins-onstar-go-the-auto-industrys-first-cognitive-mobility-platform-delivered-by-ibm-and-general-motors/.

[11] Mastercard, "Mastercard and General Motors Power Digital Payments," press release, May 2, 2017, https://newsroom.mastercard.com/press-releases/mastercard-and-general-motors-power-digital-payments/ .

4.4.1 Smart Parking

In 2016, Visa, ParkWhiz, and Honda demonstrated the connected car parking use case[12] at Mobile World Congress. The driver parks the car at a smart parking location, pushes the "park" button on the app, and leaves. The ability to pay for parking is dynamic (that is, the driver need not load a parking meter based on anticipated time); the driver pays only for the time used. When the parking session ends, the elapsed time and amount paid are displayed on a dashboard screen, and the driver selects "Confirm Payment"' to complete the transaction.

4.4.2 Paying Tolls and Parking

Long-range radio frequency identification (RFID) can transform license plates and windshield labels into electronically readable secure documents that can support authentication. RFID-enabled license plates and windshield labels can be read at a range of 10–15 meters, without the requirement for a clear line of sight or batteries, while ensuring privacy protection. A reader is needed, and the supporting infrastructure can be stationary (i.e., built into overhead gantries, parking meters, or access barriers at parking facilities). It is also possible to turn a smart phone into a reader with a simple add-on device. The reader could deduct funds from the driver's bank or other account through a secure transaction

RFID can also enhance the ability to enforce parking ordinances and provide parking availability information to the public, easing congestion and improving traffic flow on city streets.

4.5 Industrial Commerce Payments

Two use cases for industrial payments are: machines reordering replacement parts for themselves and a smart supply chain managed by industrial robots.

4.5.1 Machines Ordering Replacement Parts

Most machine parts are either replaced on a schedule (which means a part might be taken out of action well before the end of its useful life) or after they have broken. Both approaches create inefficiencies. Proposed use cases enable machines to assess the wear-and-tear on each of their parts and automatically reorder (and pay for) replacement parts only when necessary.

4.5.2 Smart Supply Chain

In fully automated assembly lines, robots can entirely manage the supply chain. These industrial robots can reorder parts for the products they are building as needed, thus maintaining an efficient supply chain and without needing human intervention in the supply chain reordering process.

4.6 Role of the Payments Networks

The payment networks, led by Visa and Mastercard, are playing a central role in fostering IoT payments. Initiatives have included:

- Helping to build the industry framework to advance availability and adoption of tokens through the use of standard specifications to ensure interoperability and payment acceptance across IoT devices.

[12] ParkWhiz, "Visa Extends Secure Payments to the Automotive Industry," press release, https://www.parkwhiz.com/about/releases/2016-02-22/.

- Developing and maintaining the technology required to enable IoT commerce, including the tokenization and digitization of credentials, card lifecycle management, and fraud/risk assessment.
- Delivering a simple and scalable commercial framework that issuers and IoT device manufacturers can use to participate in IoT programs. Programs like Mastercard Digital Enablement Express[13] expedite the process of digitizing and tokenizing Mastercard accounts.
- Forming key partnerships with IoT hardware and software vendors (e.g., secure element chip manufacturers, token service providers) and IoT device manufacturers (e.g., Honda, IBM, GM, Fitbit, Garmin), bringing entities who previously had no involvement in the payment value chain into the payment ecosystem
- Providing IoT device manufacturers and IoT token service providers with access to the network's payment card tokenization platforms to achieve scale more efficiently (for example, IoT device manufacturers were given access to Visa's VTS[14] and Mastercard's MDES tokenization platforms). Mastercard developed the Mastercard Engage program to approve digital partners connecting directly to MDES and serve as the token service provider to IoT device manufacturers.[15]
- Bringing to the market proofs-of-concept that highlight the value IoT commerce can bring to people's lives and that also test the viability of the concept.
- Developing a streamlined approval/certification process to bring IoT payment solutions to market.

Lastly, the payment networks also play a part in assessing the efficacy of various authentication methods (e.g., fingerprint, facial recognition, heart rate, voice) to protect the integrity of the payments ecosystem. Mastercard went one step further and acquired NuData, a company that specializes in IoT security.[16]

[13] Mastercard, "Mastercard Launches Digital Enablement Express Program to Speed the Global Rollout of Digital Payment Services for Consumers," press release Sept. 8, 2015, https://newsroom.mastercard.com/press-releases/mastercard-launches-digital-enablement-express-program-to-speed-the-global-rollout-of-digital-payment-services-for-consumers/.

[14] http://www.businesswire.com/news/home/20161025005672/en/Visa-Opens-Tokenization-Services-Party-Partners

[15] Kiki Del Valle, "It's Time to ENGAGE with all our Digital Partners," Mastercard, Sep. 6, 2017, https://newsroom.mastercard.com/2017/09/06/its-time-to-engage-with-all-our-digital-partners/.

[16] Mastercard, "Mastercard Enhances Security of the Internet of Things with the Acquisition of NuData Security Inc.," press release, Mar. 29, 2017, https://newsroom.mastercard.com/press-releases/mastercard-enhances-security-of-the-internet-of-things-with-the-acquisition-of-nudata-security-inc/.

5 Security Threats to IoT Payments

The security threats posed by the use of IoT devices for payments are serious concerns for all stakeholders in the ecosystem. This section discusses potential security issues.

5.1 Current Security Issues

IoT device security. One major concern with using IoT devices for payment is the security of the device itself. IoT devices have small amounts of memory and limited processing power, making it difficult to use current, well-established security protocols and to push regular security updates (such as firmware updates) to the devices. When devices are powered by a battery, remote security updates are even more challenging, since power must be conserved to prolong the life of the devices.

Data leakage and privacy. The threat to privacy is exacerbated by IoT devices' low resistance to data leakage. IoT payments have the potential to generate large amounts of data about personal spending habits, representing a potential target for cyber criminals. Stolen data is likely to contain personal information that can then be used for unlawful surveillance and tracking users.

IoT devices and distributed denial of service (DDOS) attacks. IoT devices present a platform for launching DDoS attacks. Recent events[17,18] have shown that some of these devices are shipped with no protection. Default credential settings and open remote access make it easier for attackers to take over the device remotely. Typically, IoT devices require minimal or no user interaction, which makes it even more difficult for the users to tell when their devices are under attack.

5.2 IoT Payments Characteristics

Certain characteristics of the IoT payments use case may have an impact on security.

Autonomous and invisible payment. Many IoT payments scenarios only make sense if transactions occur invisibly or autonomously—that is, with no direct user interaction. However, user authentication is an important part of the security architecture of the traditional payments infrastructure. There is therefore a need for effective user delegation and authorization mechanisms.

Payment device identity. Arguably one of the most important factors in securing IoT payments is an immutable way of identifying the device. Reliable identities enable devices to establish trust, communicate with each other, and also to send out data with confidentiality and integrity. In most cases, public key cryptography will be the most feasible security technology used to interact with IoT devices. The public key infrastructure (PKI) depends on assurances that the sender of an encrypted message is indeed the owner of the key pair.

Payment liability. Finally, when there is a dispute or erroneous payment, who takes responsibility? Both unique device authentication and strong delegation and user authorization mechanisms will go a long way toward solving this problem.

[17] Infosecurity Magazine, "Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack," Jan. 3, 2017, https://www.infosecurity-magazine.com/news/leet-iot-botnet-bursts-on-the-scene/.

[18] Ben Herzberg, Dima Bekerman, Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," Imperva Encapsula, Oct. 26, 2016, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

5.2 Tokenization for IoT Payments

Tokenization appears to be the currently preferred approach for securing payment account information in IoT payment transactions.[19,20] The following issues should be considered when implementing tokenization with IoT devices.

- Secure capture of the card information to be tokenized
- Response to subsequent token requests
- Validation of the token
- Risk of skimming for small value transactions

For tokens to be provisioned to a device, the card to be tokenized must be captured. This is the step in which the primary account number (PAN) is potentially vulnerable. A secure capture path is mandatory to ensure that the PAN is not exposed.

Subsequent token requests are also vulnerable to exposure and abuse. EMVCo mandates a user identity and verification (ID & V) step before granting any token request. A similar mechanism is necessary to ensure that device owners are aware of token requests originating from their devices and that such requests are legitimate.

Another consideration is how long a token should remain valid. The length of time a token remains valid is typically based on the level of perceived risk. Tokens in high risk environments will have a shorter validity period.

With a sharp rise in the magnitude of IoT devices used for DDOS attacks. It is conceivable that networks of IoT devices will be compromised in order to perform fraudulent transactions that add up to a greater value. Many devices can team up to skim trivial amounts of money that users will have difficulty detecting. Another example of small value attacks that could avoid detection is to set up a false road tolling device and take a few cents from every car that passes.

[19] Visa, “Visa brings secure payment solutions to the Internet of Things,” https://usa.visa.com/visa-everywhere/innovation/visa-brings-secure-payments-to-internet-of-things.html.

[20] Mastercard, “Mastercard Launches New Program that can Turn any Consumer Gadget, Accessory or Wearable into a Payment Device,” press release, Oct. 26, 2015, https://newsroom.mastercard.com/press-releases/mastercard-launches-new-program-that-can-turn-any-consumer-gadget-accessory-or-wearable-into-a-payment-device/.

6 Considerations for Designing Payments-Enabled IoT Systems

The current IoT payments implementations described in this white paper share many similarities with traditional payment processes. The transaction flow can be the same as the EMV flow at a physical retailer (for example, using a wearable at the POS) or the transaction can resemble an e-commerce transaction (a card-on-file transaction). Like NFC-enabled mobile payment devices, IoT payment devices are provisioned with payment tokens and use the tokens for payment transactions.

However, IoT payments are significantly different from traditional payment processes. The IoT device itself is the payment instrument (it stores the payment credentials locally or connects to the cloud to use remotely stored credentials). Before implementing IoT payments, consider the following:

- A physical POS device is not required for the payment process. The transaction can be routed directly to a network by any IoT device (a mobile phone, connected car, or Internet-connected TV or appliance).
- The customer can be recognized automatically using an IoT technology such as smart sensors.
- The customer experience in initiating a transaction will vary based on the IoT device and use case (e.g., a contactless tap with a wearable vs. a voice command with a home assistant).
- Data analysis and sensors can be used to send smart offers to the customer.
- The customer identity may be verified using biometric or other technologies.
- The payment card credentials can reside on a variety of hosts, including a secure element, the cloud, or software using host card emulation.
- Devices must be online at some point for provisioning and lifecycle management. Provisioning the payment credential may depend on the use case and device technology.
- A different approach to branding is required to keep the relevant payment brand prominent on an IoT device.
- IoT payments move from the closed, controlled payment networks to public networks, entailing use of different technologies and infrastructure. Additional industry participants support the IoT payments infrastructure.
- There is a wide variety of IoT devices. Some IoT devices have limited capability, and different devices can connect to the payment network in different ways. IoT devices do not all have the same resources and potential for customization.
- All IoT devices do not have sufficient capabilities to support security for the payments use case. Not every device can be trusted. For example, the automotive industry worked to assess and set requirements for IoT device ability to support required security.
- The device authentication model may vary from device to device. An adaptive or continuous authentication model (for example, a model that looks at a confluence of factors such as device identity and location) may be more relevant for less secure devices.
- The trust model varies with varying IoT device security capabilities and approaches and the potential need for third-party services.

This section looks at a few of the considerations outlined above:

- Enabling the consumer experience
- Implementing security
- Managing the device lifecycle

6.1 Enabling the Consumer Experience

Today, consumers browse and complete transactions using multiple channels and increasing numbers of connected devices. Consumers are therefore looking for a unified experience that transitions seamlessly between the digital and the physical environments. Merchants and financial institutions that serve consumers directly must bridge the physical and digital worlds on behalf of their customers.

Consumers are also becoming more aware of their digital footprint and want more control over it. Expansion of the IoT greatly increases that footprint, especially as the industry moves from the world of "single device and single experience" to an ecosystem of multiple connected touchpoints. As customers move toward greater convenience, it is critical that security not be sacrificed. Consumers can be protected through (for example) the use of tokenization to protect card data from fraud, or by using biometric or behavioral authentication.

In addition, a new form of consumer "value exchange" is emerging. Consumers may be willing to share information with selected third parties through a connected device in return for a tangible benefit. Examples of value exchange include United Healthcare's wellness program, called Motion, which allows users to earn up to $4 a day in credits for reaching fitness goals tracked by a Fitbit device.[21]

6.1.1 Consumer Experience Considerations

Designing the consumer's IoT payment experience is complicated by the variety of IoT devices in use.

Certain portions of the user experience are relatively device independent:

- Card information entry (either via a form or initiated by the OEM if provisioned by the issuer)
- Identification and verification (ID&V) process (with issuer validation and processes for step-up validation, if needed)
- Tokenization, including the ability to suspend/delete tokens
- Branding requirements

However, other considerations are device-dependent, including:

- What type of transaction is required (offline or contactless as opposed to remote).
- The complexities of building merchant acceptance (for example, will the device support contactless payment at the POS or require new POS technology).
- The relevancy of different use cases. For example, research shows that consumers in a car are looking for four use cases only: tolls, ordering ahead, parking, and fuel. There is no need to provide solutions for all use cases.

[21] Elizabeth Gurdus, CNBC, "UnitedHealthcare and Fitbit to pay users up to $1,500 to use devices, Fitbit co-founder says," Jan. 5, 2017, https://www.cnbc.com/2017/01/05/unitedhealthcare-and-fitbit-to-pay-users-up-to-1500-to-use-devices.html.

- Emerging business models for the sharing economy and different IoT use cases.
- Requirements for identification and authentication to safeguard consumer credentials.

Mobile devices play a critical role. For example, automobile OEMs should think of the connected car as a commerce platform with multiple consumer touchpoints. Moreover, auto manufacturers increasingly want any vehicle a user enters to be personalized to the user's preferences; therefore, implementation needs to account for both the sharing economy and autonomous vehicle use cases. (Even a single-owner vehicle may require personalization to accommodate different drivers within the owner's family.)

6.1.2 Consumer Experience and Trust Models

Consumers rely on a trusted intermediary to enable a service experience. Currently, consumers enable an IoT payment experience by expanding an existing business relationship to include new or enhanced service. The consumer simply trusts that someone will ensure service quality and security and create a seamless experience.

Traditional trusted intermediaries include the following:

- Financial service providers (banks, brokerages, insurance agents, creditors)
- Government services (national or regional authorities for tolling, identity, taxes, transit)
- Communications (telephone) and Internet service providers

The trusted intermediary is responsible for designing an extended service model that provides payment capabilities in addition to other services. By developing models supporting IoT devices, such as cars, the service provider can expand their relationships with their customers, leveraging the current trusted relationship to include the expanded service offerings.

As customers seek to take advantage of the benefits of IoT payments, differing expectations of trust, privacy, and security suggest two distinct service models:

- Identifiable, or account-linked
- Anonymous, or intermediary service or object-linked

Interacting with the Internet implies public connectivity. Customers who trust a provider will typically establish an account and provide some form of guarantee for their transactions through verification of their personal identity. Because this is the most common way of enabling an Internet interaction, banks, government agencies, and telecommunication providers are leaders in the area of service provisioning. These entities have trusted relationships with consumers and can build an ecosystem to deliver a better consumer experience. For example, Apple formed relationships with the banks and payment networks to deliver phone-based transactions.

However, because consumers value private transactions, other, anonymous models can emerge. A community of block-chain acceptance providers can serve as an intermediary service provider and support anonymous purchases by linking value to an object, rather than an account. Another early successful example is the use of contactless preloaded smart cards to pay for public transit. The cards can be reloaded at ticket vending machines, providing for anonymity compared to a customer who has decided to create an account and share some level of personal information with the transit provider.

In both cases, an intermediary account with a trusted service provider can enable customers to use an IoT device for payment. The intermediary, not the consumer, designs and manages the technical and business relationships. The only difference is that in one case, the payment service is linked to an account and in the other it is not.

6.2 Implementing Security

IoT devices are connected to the Internet, opening the door to every type of Internet threat and attack—to capture sensitive information, take control of the device, and use the device for attacks such as DDoS attacks.

6.2.1 Storing and Securing Data

The integrity of IoT commerce depends on the integrity and authenticity of payment-related data, specifically the payment token, cryptographic keys, and authentication data (for device and cardholder verification), and on the communication channels used to facilitate the payments process. Consequently, where the credentials and keys are stored and the mechanisms used to cryptographically secure the storage location are critical.

There are three possible storage locations:

- **On the IoT device**. The IoT device can secure the payment or authentication credential and cryptographic keys in a tamper-proof location. Protecting data at rest requires a strong, certified security module, such as a secure element (SE). The SE—a tamper-resistant secure micro-controller—provides an ideal platform for implementing required security functions and ensuring that credentials are stored in a secure environment. Another hardware mechanism for protecting data at rest on the device is the relatively secure Trusted Execution Environment (TEE).

  While hardware-based mechanisms provide better security, depending on context, certain IoT devices may rely on less secure but more practical software storage, protecting data through techniques such as code obfuscation.
- **In the cloud**. Certain IoT payment implementations can rely on credentials stored in the cloud or implement a card-on-file type of payment. In this case, the payment token and cryptographic keys are stored in the cloud, where it is easier to protect data. The communication channel used by the IoT device to identify itself to the cloud must be secure.
- **On a different device**. Certain implementations could provide a true connected device payment experience in which IoT devices in a particular environment leverage the secure payment and authentication capabilities of another connected device (such as a smartphone) in the same environment.

It is also important to consider how to secure sensitive data in transit. While some IoT devices can be provisioned with payment credentials before being released to consumers (for example, a passive prepaid wearable), most IoT devices require secure provisioning in the field. As a result, data must also be protected in transit, and a secure channel is needed to manage the credential lifecycle (e.g., to deactivate or upgrade).

As discussed in Section 5.2, the payment tokenization infrastructure is being used to securely create and manage payment credentials on IoT devices, including:

- Generating the token that replaces the actual payment credential
- Verifying and authenticating the device that will host the credential
- Securely delivering a unique payload to the device to provision the credentials
- Securely managing the lifecycle of the payment credential

6.2.2 Device Authentication

A fundamental requirement in the payment process is the need for simple but trusted, secure methods to authenticate an IoT device and for devices to authenticate the party with whom they're communicating. The traditional EMV payment process uses dynamic data generated during the transaction; the issuer validates this data came from an authentic device when authorizing the transaction. Many of the use cases described in this white paper also use this process.

New use cases need to consider how to create the root of trust and implement device authentication. In addition, many IoT device authentication methods (such as embedded sensors) rely on machine-to-machine processes with no human intervention. Machine-to-machine processes require anonymous entity authentication solutions that can execute efficiently on a wide range of resource-constrained IoT devices. Such interactions require new authentication methods, protocols, and standards.

6.2.3 Consumer Authentication

In a traditional card payment, the cardholder identity is verified with a signature or PIN; with many low-value transactions, no cardholder verification is required. Payment using IoT devices will use new forms of consumer authentication and expanded use cases for authentication.

6.2.3.1 Consumer Authentication Methods

The following are examples of consumer authentication methods that may be used with IoT devices.

Voice recognition offers one approach to consumer authentication. IoT voice technology is evolving; voice recognition functionality is no longer restricted to a central hub but can be provided by the individual networked devices that are part of the IoT. One-touch NFC commissioning, that allows users to connect systems intuitively through a single tapping motion, supports the installation and connection of IoT devices that support a variety of networking standards, including ZigBee 3.0, Thread, and Bluetooth Low Energy, enabling the user to control conventional “edge” devices such as smoke detectors and fire alarms.

Another method of authenticating an individual is **heartbeat**. Like a fingerprint, each individual's electrocardiogram (ECG) pattern is unique. A major benefit of using an ECG for authentication is resistance to replay attacks and spoofing. Wearables have already been developed that use an ECG for authentication. One such device, the Nymi Band, only unlocks the keys it stores for authentication after the wearer's ECG is validated against the stored template.

NFC technology is another option for authenticating consumers to a device for IoT related payments applications. Over the past two years, several major payments companies have embarked on plans to leverage NFC to enable all sorts of consumer devices, such as key fobs and wristbands, to execute payments. The secure payment functions can be added to a companion app on a wristband (for example), enabling the wristband to conduct the transaction.

In addition, an IoT environment may enable an individual to authenticate to multiple devices, all located nearby, simultaneously. The individual can then be authenticated biometrically using different modes. The biometric authentications can be proven to have occurred at the same time and in the same place to authenticate the individual in real time. The chances of ensuring a positive identification using this layered approach are extremely high and remove the risk that loss, theft, or compromise of one item in this chain of authentication will result in a threat to security or privacy.

6.2.3.2 Authentication Protocols

A variety of methods permit an issuer to authenticate an IoT device or consumer. Which method is used typically depends on the context in which the consumer is being authenticated.

Thousands of issuers cannot manage the wide variety of context-sensitive device or consumer authentication methods at the host. Individual issuers cannot feasibly evaluate the veracity of the variety of authentication methods. Widespread adoption of and participation in the IoT commerce ecosystem therefore requires that issuers be provided with a scalable mechanism to use to authenticate IoT devices and consumers. The protocols used to manage authentication, regardless of the underlying authentication method, are vital.

This section highlights three authentication protocols that could prove useful for IoT commerce. These protocols are not mutually exclusive, and, in fact, the different consortu fostering their adoption are working with each other to ensure interoperability.

The first protocol, the FIDO Universal Authentication Framework (or UAF), provides strong authentication through public key cryptography. The protocol is meant primarily to avoid the use of static authentication mechanisms, such as passwords or PINs. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is accomplished by the device signing a challenge that proves possession of the private key. The private key can be used only after the device's user unlocks it by an action such as providing a fingerprint to the device, entering a PIN, speaking into a microphone, inserting a second-factor device, or pressing a button.

EMVCo published specifications for a second protocol, 3-D Secure 2.0, in 2016. 3-D Secure (3DS) is a messaging protocol that enables consumers to authenticate themselves to a card issuer when performing card-not-present (CNP) transactions. 3DS is meant to work with a variety of authentication methods. It enables intelligent, risk-based decision-making, encouraging frictionless consumer authentication. In October 2016, Visa announced that Intel[22] will use the 3DS protocol to provide issuers with hardware level data (a "secure device code") during authentication. The announcement also stated that 7th Gen Intel® Core™ vPro™ systems will incorporate the 3-D Secure protocol.

The third protocol, OpenID Connect, is an identity layer on top of the OAuth 2.0 authorization protocol. It allows clients to verify the identity of the end user based on authentication performed by an authorization server and to obtain basic profile information about the end user. OpenID Connect allows clients of all types, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end users. The specification suite is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID providers, and session management.

6.3 Managing the Device Lifecycle

The main point to remember in managing the lifecycle of IoT devices is that another device in the same environment may not have the same security needs as the IoT device used for payments. This other IoT device usually has not implemented the strict security needed for payment credentials. Therefore, the

[22] Visa, "Visa and Intel Collaborate to Drive Better Payment Security for Connected Devices," Oct. 24, 2016, http://investor.visa.com/news/news-details/2016/Visa-and-Intel-Collaborate-to-Drive-Better-Payment-Security-for-Connected-Devices/default.aspx.

IoT payment device must ensure all communications and processes for management are secured end-to-end, from the security component to payment issuer backend system.

The specific manufacturing and distribution models, as well as the day-to-day usage, of IoT devices represent a significant change for lifecycle management compared to other payment devices. The diverse capabilities mean that one model for lifecycle management will not work across all devices. However, there are similarities in fundamental characteristics that can be applied to all models.

Work is underway to provide lightweight versions of the processes and systems described in this section. Managing the lifecycle of IoT devices has unique challenges since they are part of a heterogeneous environment and have an extremely wide range of capabilities. This section provides some specifics that are applicable across most, if not all, IoT devices, with the caveat that the security and processing requirements may be lower than what is required currently.

IoT devices may not have any over-the-air (OTA) management capabilities. These are usually wearables with very limited system resources. Lifecycle management for these devices follows the same process as traditional payment credentials using a physical interface.

Most IoT devices have an OTA interface that can be used for managing the device. OTA provides more flexibility but also incurs new risks. The IoT devices must have robust communications and security systems to handle the transfer of sensitive information, like the payment credentials. The main advantage is that the device distribution and management processes are decoupled.

Through OTA, both the loading of the payment application and the provisioning (also called personalization) of the application can be performed. Provisioning is examined in Section 6.3.1 and application loading is covered in Section 6.3.2.

6.3.1 Provisioning

Usually the main part of the payment application is loaded on the IoT device before it is distributed. Provisioning of this application makes it useable, as in the base payment application is personalized for a specific bank and customer. The OTA interface establishes a secure channel with the application issuer (i.e., the credit card institution) in order to keep the information secret and secure, and ensure it is transferred completely.

IoT devices using a secure element (SE) must initiate the secure connection, and therefore must be triggered to make this connection. This trigger can be accomplished through a user application on the IoT device or a notification sent from another system. The SE establishes connections only to a secured system, called a Trusted Service Manager (TSM), that can be properly authenticated. Further details of these methods and systems are beyond the scope of this paper. The GlobalPlatform specifications detailing these mechanisms can be found at https://globalplatform.org/specificationsdevice.asp under “Secure Element Management.”

IoT devices using a Trusted Execution Environment (TEE) or Host Card Emulation (HCE) have similar options to the SE above. The main difference is the initiation of the provisioning process. The banking applications can either personalize the trusted application directly or can act as a proxy to the application issuer’s Internet systems.

The connection between the banking application and the trusted application is provided by the TEE and HCE specifications, which also define the types of security used. When acting as a proxy, connection security (i.e., TLS) must be used. Caution should be used as TEE and HCE systems use only software-based security. The use of tokenization helps in limiting the risk in using software-based security.[23]

6.3.2 Installing and Upgrading Applications

Traditionally the base payment application is installed onto the IoT device before it distributed to the customer. This requires the payment application issuer to have access to the IoT device before it is distributed. This traditional process is changing, since the distribution of the IoT devices is done independently of the payment application issuer.

6.3.2.1 Loading an Application on the SE

The payment application can be can be downloaded and installed after the IoT device is distributed to the customer. A TSM with the appropriate privileges is required to load the payment application onto the SE. It is recommended that the payment application be encrypted and signed to ensure the application received is the same that was sent. Further details on the TSM and the mechanism to connect to and load the file on the SE can be found in the GlobalPlatform System Specifications at https://globalplatform.org/specificationssystems.asp.

6.3.2.2 Upgrading an Application on the SE

Payment applications may also need to be upgraded during the IoT device's lifecycle. The steps required to do this traditionally include:

- Saving the personalization data
- Removing the instances and the application
- Loading the new application and installing the instances
- Restoring the personalization data to the instances

The main issue with this process is saving the personalization data and reloading it after the new file is installed. GlobalPlatform has released Amendment H for upgrading the SE payment application. This amendment introduces a new command that executes the upgrade steps, including saving and reloading the personalization data. Amendment H is available for download at https://globalplatform.org/specificationscard.asp.

6.3.2.3 Loading and Upgrading an Application on a TEE

The TEE requires a Trusted Application Manager (TAM) with the proper privileges to load applications. A TAM uses a system-level application on the IoT device that acts as a proxy. The TAM either installs the system proxy with the installation of the TEE or through an agreement with the IoT device manufacturer. The payment application issuer uses the services provided by the TAM to install the payment application, similar to a TSM for the SE.

The trusted application has to be in the "executable state" to be used by the banking application. The trusted application is put into the "locked state" for it to be upgraded. After it is upgraded, it is returned to the executable state. The application provider is responsible for any personalization data being used by the trusted application.

[23] For additional information, see the Secure Technology Alliance white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," https://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

6.3.3 Lifecycle Changes

Device manufacturers and service providers need to be aware that even after the device has been delivered to the end user and the payment credential has been provisioned, there is still a need to manage the lifecycle of the payment application and the IoT device itself. Key considerations include:

- Ownership change
- Expiration of payment credentials
- End of life

6.3.3.1 Ownership Change or Expiration of Credentials

IoT devices will invariably change owners during their lives. As a result, the personalization data and security keys could potentially be exposed to the new owners. The original payment application issuer has to provide mechanisms to request or detect the ownership change. A request can be either through the IoT device user interface or through a new device proxy (for example, a home gateway). Detection can be done through the new device proxy or through a back-end system change.

When the ownership change has been requested or detected, the payment application issuer will remove the personalization data for the application and, optionally, the payment application itself. The payment application issuer has the option to deactivate the SE application (“unelectable state”) and TEE application (“inactive state”). The TEE can also be reset, which will remove all applications not saved by the TAM. It should be noted that the TAM can choose to save the trusted payment application.

The payment application issuer should rotate the keys when ownership changes. Key rotation installs a new set of security keys, ensuring the new owner is not using the original owner’s keys.

If the IoT device ownership change is detected and can no longer be managed by the payment application issuer, the personalization data and security keys should be deemed to be compromised. The payment application issuer should treat the credentials as a stolen.

6.3.3.2 End of Life

When the IoT device has reached its end-of-life, the IoT device manufacturer or payment application issuer can terminate the life of the trusted components. In the SE, the transition to termination is permanent. The TEE does not have a permanent state, as such.

The SE can enter the “terminated state.” In this state, only a designated application will respond to a general query, a status request. No application will run and no secure connection can be established; this state cannot be reversed. As an SE is required to be separated from the rest of the device components, this ensures that nothing is gained by disassembling the IoT device.

The TEE itself can be put into the “locked state.” However, this state can be reversed. The TEE can also be reset, which removes all applications and their data except for the applications specifically set to remain. As the TEE runs on the secure part of the IoT device processor, it can always run as long as the processor can run. A better scenario is to deactivate the IoT device processor.

7 Conclusions

The next generation of interconnected devices promises to be commerce-savvy. IoT devices will play a significant role in the day-to-day activities of the consumer, whether it be the refrigerator ordering milk before the carton is empty or the car paying for its own parking.

This white paper focused on IoT payments that leverage the traditional payment infrastructure and on early use cases and pilots. Several categories of IoT commerce uses cases that have emerged thus far are: connected cars, smart home appliances, wearables, virtual or augmented reality devices, industrial devices, and retail. IoT payments have the potential to extend beyond this traditional approach in the future and leverage new decentralized technologies (e.g., blockchain) and device-to-device capabilities.

The reality is that IoT commerce and IoT payments are currently still in their infancies. A majority of IoT devices do not have the ability to engage in commerce, much less imbed the ability to conduct secure payments. The future of IoT commerce depends not only on the creation of use cases that solve a customer problem or improve the consumer experience, but also on the IoT economic ecosystem's ability to create and sustain trust in the ability to perform commercial transactions using an IoT device.

8 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance IoT Security Council and Payments Council to provide a resource for the industry that outlines the current market landscape for implementing payments with IoT devices and provides guidance for developing IoT applications that will include payment.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development of this white paper included: American Express; Cardtek; Consult Hyperion; CPI Card Group; Discover Financial Services; Entrust Datacard; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Ingenico; Initiative for Open Authentication (OATH); IQ Devices; Mastercard; Metropolitan Transportation Commission (MTC); NextgenID; NXP Semiconductors; Rambus; Underwriters Laboratories (UL); Visa.

The Secure Technology Alliance thanks Council members who participated in the project team to write and review the document, including:

- **Andreas Aabye**, Visa
- **Stephen Abbanat**, MTC
- **Philip Andreae**, IDEMIA
- **Alyssa Arredondo**, Entrust Datacard
- **Vishal Bhatt**, Discover Financial Services
- **Charl Botes**, Mastercard
- **Ilker Caner**, Cardtek
- **Hank Chavers**, GlobalPlatform
- **Brady Cullimore**, American Express
- **Laurie Dornberger**, CPI Card Group
- **Jon Ferguson**, Entrust Datacard
- **Allen Friedman**, Ingenico
- **Melanie Gluck**, Mastercard
- **Jack Jania**, Gemalto
- **Ranjeet Khanna**, Entrust Datacard
- **Tom Lockwood**, NextgenID
- **Mina Malak**, G+D Mobile Security
- **Don Malloy**, OATH
- **Cathy Medich**, Secure Technology Alliance
- **John Neal**, NXP Semiconductors
- **Nick Norman**, Consult Hyperion
- **Keith North**, CPI Card Group
- **Nick Pisarev**, G+D Mobile Security
- **Steve Rogers**, IQ Devices
- **Srinath Sitaraman**, UL
- **Jason Soroko**, Entrust Datacard
- **Mateen Syed**, Discover Financial Services
- **Fatih Teksoy**, Cardtek
- **Christopher Tomczak**, Discover Financial Services
- **Nicholas Vondrak**, IDEMIA
- **David Worthington**, Rambus
- **Stephane Wyper**, Mastercard
- **Mike Zercher**, NXP Semiconductors

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

About the Secure Technology Alliance IoT Security Council

The Secure Technology Alliance IoT Security Council was formed to develop and promote best practices and provide educational resources on implementing secure IoT architectures using "embedded security and privacy." The Council focuses on IoT markets where security, safety and privacy are key requirements and will leverage the industry expertise and knowledge gained from implementing embedded security technology for payment, identity, healthcare, transport and telecommunications systems to provide practical guidance for secure IoT implementations. The Council provides a unified voice for the industry to the broader IoT ecosystem.

Additional information on the IoT Security Council can be found at https://www.securetechalliance.org/activities-councils-internet-of-things-security/.

About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.