The following use-cases are described in detail in this paper:

USE-CASE #	
UC1	Mitigation of new cryptographic flaws or vulnerabilities
UC2	Compliance to local laws, regulations, or standards
UC3	Amortization of Industrial IoT
UC4	Platform Design: build once – fly/float/roll anywhere
UC5	Cloud Services: build once - run anywhere
UC6	Interoperability

For a long time, cryptography was merely something we were asked to use, in the context of an information security program. "Set it and forget it" (apologies to the Ronco Rotisserie) was the standard of the day. It did not really matter what type of crypto was used, because at the time it was all assumed to be sufficient. But with most things, times have changed: cryptography is now something that must be managed, not just implemented and forgotten.

When we say "managed", we mean in the sense that is must be carefully selected, implemented, maintained, and retired from service according to requirements such as:

- *the information it protects;*
- *the length of time that information needs to remain secret or secure;*
- *the platforms it must operate on;*
- *the regulatory environment it operates within;*
- *newly discovered vulnerabilities and mathematical attacks; and*
- *the emergence of quantum computers at a sufficiently strong scale to threaten classic cryptography.*

Managed cryptography is the opposite of the "set it and forget it" implementations that are the norm. In most cases, cryptography has been hard-coded into operating systems and applications by manufacturers and left in place, forever. This static profile makes it difficult, if not impossible to change if any of the above requirements change or evolve, leaving the underlying cryptography, and by extension, the system or application that relies on it no longer fit or compliant.

Managed cryptography is exemplified in "agile cryptography" as we mentioned earlier: the agility to implement, update, change and remove cryptographic functions from systems and applications on demand, without changing the systems or applications themselves. Cryptographically agile systems are dynamic and able to adjust to changing requirements, including new threats.

Agility Today

Many operating system vendors today (Microsoft, Apple, Google, etc.) have some measure of intrinsic agility through their integrated software update processes. But these usually require the downloading of large update packages and rebooting – and only support their products directly. Adding to that is the fact that this process is largely manual or opt-in, making deployment of critical updates slow at best. This says nothing to third party products that rely on crypto built into the operating system that may need to rebuild their products to support those updates, and again requiring the end user to manually update.

In-house applications are often completely static from a cryptographic perspective, lacking any agility whatsoever. Typically, updates to in-house cryptographic implementations to address threats or vulnerabilities will require complete code updates, QA testing, and reinstallation if updates are possible at all; developers of in-house applications may have retired, or otherwise moved on, leaving behind an unknown state for other developers to try to wade through.

Hardware Security Module (HSM) vendors allow some form of agility – as long as you load the crypto into their specific hardware, using their specific import toolkits and go through the necessary key-generation ceremonies and processes, which is no minor task. But even this is no panacea: not all applications need, or can even use, HSMs.

In 2018 and 2019, there are some pioneering, but nascent and incomplete discussions around "cryptographic agility". For instance, Agile certificates in the context of Public Key Infrastructure are regularly discussed. These typically refer to certificates that contain two forms of public key and signature: a classic public key and a post-quantum public key. These keys will have some shared attributes – like the Subject Name potentially – and also dual Certificate Authority (CA) signatures – again, one signature based in contemporary (classic) cryptography and one post-quantum based on cryptography. (The discussion to following will summarize the risks to classic crypto posed by quantum computers). Agile certificates are not so much agile, as they support a binary choice of classic or post quantum crypto from a single certificate. Agile certificate are an improvement and do offer the ability to choose from two different generations of cryptography – but they still rely on the applications and devices having the cryptographic functions on-board to use the certificates. What is more, an application or device could use so-called "agile certificates" but in fact be entirely static from an cryptographic perspective: all features and functions are hard-coded and unchangeable.

Finally, early forms of cryptographic policy management tools have started to appear in the operating system market, though focused again on managing statically compiled, classic cryptography. In this case, the tools appear to allow rules to be applied around what type of available crypto on a systems might be used by an application or system. For instance, it is very common for applications to have direct access to a lot deprecated and insecure cryrpto built into its base operating systems (and never removed). This means you are never more than an administrative oversight away from deploying weak or deprecated crypto. Ideally, the system policy will enforce rules forbidding that crypto from being used. How the policy is enforced is a different matter and beyond the scope of this paper.

Risks Facing Cryptography

Classic cryptography means the crypto we have been using for up to 30 years. Looking at it another way, classic is just a nice way of saying old. But unlike like classical music or Classic Coke, a lot of that classic crypto is weak or vulnerable, and the remainder of it will be good for an unknown period: current thoughts are somewhere between 5 and 20 years. What are some of the risks entwined with continuing to use classic cryptography?

Risk #1 – Awareness

Awareness of the existing or changing risks associated with aging, classic crypto is possibly the largest risk of all, because risks surrounding crypto remain largely misunderstood or ignored. Crypto is frequently seen, even by seasoned technical professionals, as too complicated to approach and therefore someone else's problem.

Crypto was both static and unchanged since the early 1990's and the balance of threat and risk has only really tipped towards response recently. If we were looking for a watershed moment, we might consider the revelations associated with the Snowden leaks in 2013. At that time, the power of intelligence agencies to hack and eavesdrop became widely known, and all conventional security tools and systems became suspect. Perceptions, standards and laws started to change as a result – but undoing 25 years of habit takes more than 5 years – bringing us to 2019.

In a nutshell: cryptographic agility is a term every executive needs to learn.

Risk #2: Changing Audit Criteria

Since 2013, most of the largest and widely applied cyber security standards such as ISO, CoBIT and NIST have undergone major revisions related to the use of cryptography. Specifically, they have started to ask fundamentally different questions about crypto. Formerly, they would ask: "Are you using crypto?". Now auditors ask: "Are you using good crypto?" The distinction is between setting and forgetting about crypto (or worse: letting your vendors set it and forget it for you) and managing all the cryptography in use inside your organization. Additionally, laws and regulations, while often slow to adapt to technological change, are becoming much more prescriptive as well. They are also demanding that organizations not just use cryptography but use good cryptography in the hopes of stymying the impact of breaches of customer data.

As a result of both of these changes, the audits against standards and regulations will be looking for evidence that management has an inventory of where crypto is used, what risks or threats have been identified, and what remediation steps are in place to deal with them. Having answers to these questions will be crucial going forward.

Risk #3: New Analytics Against Crypto

Much of the crypto that was standardized about 20 years was assumed to be highly secure and the chances of new attacks against them was considered low. In reality, much of the symmetric key (RC2, RC4, DES, 3DES) and hashing functions (MD2, MD5, SHA1) from the late 90's and 2000's have been successfully broken with new mathematical analytics. While the asymmetric key algorithms like ECC and RSA have so far held up under mathematical analysis, and some of the symmetrics like AES are still considered safe – there is no guarantee that they too will not fall in the face of constant research and crypto-analysis. And let's speak nothing of the conspiracy theories that these too may have fallen to the cryptographic analysis experts employed by nation-state agencies.

Risk #4: Implementation Flaws and Side Channel Attacks

Several devastating vulnerabilities have been found in implementations of crypto that led directly to the compromise of the crypto itself. In such cases, the algorithms themselves have not been found to be weak, but the way they were implemented in software libraries or how the keys were managed in memory led to compromises. Generally speaking, because crypto is consumed by applications through the interfaces offered by libraries, protocols, and hardware – flaws in these surfaces are tantamount to cryptographic weakness. The end result is the same: comprised systems and information.

The two most famous incidents in recent years are Heartbleed and Spectre. Heartbleed was an implementation of the very widely used protocol stack OpenSSL. OpenSSL contained accidental flaws introduced by a developer that allowed the credentials used to establish cryptographic security to potentially be exposed to a remote attacker. Worse yet, Heartbleed allowed an attacker to not only capture credentials, but literally anything you can imagine out of the memory of the victim device: emails, keys, transaction data, and all sorts of sensitive data was put at risk. Because OpenSSL is fully and tightly integrated with crypto algorithms, it was viewed as a vulnerability that encompassed cryptography, and rightly so. The only solution was to replace the OpenSSL libraries and cryptographic provider with an updated version or migrate to a different product altogether; no simple task for many organizations who lacked visibility into where OpenSSL was being used throughout their environments. Similarly, Spectre was essentially a side-channel attack associated with flaws in the management of central processor memory management in both x86 and ARM architecture chips (that is to say – almost all chips relative to the market). Spectre allowed for sensitive information stored in processor memory to be accessed by unapproved applications in user-space – including secret cryptographic keys.

Other forms of side-channel attacks include timing attacks – where the observable movement of data in and out of memory betrays just enough information about the secret keys to narrow down the potential range of keys to the point that brute-force guessing becomes practical. Similarly, power analysis attacks can serve to extract the same partial information and greatly reduce the effort required to break cryptography. Countermeasures to side-channel attacks can be deployed within the cryptographic implementations, but as defences against side-channel attacks evolve, so too do vulnerabilities.

Risk #5: Custom or Sovereign Crypto

Around the world, cryptography is become more diverse and fragmented, not less. Countries are releasing their own forms of classic cryptography in response to decaying trust in the most conventional and widely used crypto such as the Suite-B Elliptic Curves, RSA, AES, and other asymmetric and symmetric ciphers.

The risks to the use of established cryptography in the face of new sovereign crypto is two-fold:

1. If the sovereign cryptography that replaces conventional cryptography inside applications is not good. If it turns out to be flawed, weak (either intentionally or unintentionally), or vulnerabilities are discovered after it is deployed, customer data may be put at risk.
2. Companies and their applications or services using cryptography suddenly find themselves in a non-compliant position while operating inside some jurisdictions. This makes them vulnerable to sanctions and forms of lawful access requests that effectively strip away all cryptography, exposing sensitive information in a manner that might as well amount to a cryptographic failure.

SOME EXAMPLES OF SOVEREIGN CRYPTOGRAPHY AROUND THE WORLD

Figure 1: A sample of national cryptographic algorithms or standards

Risk #6: Faster Computers and Quantum Threats

The constant increase in processing power, reduction in the costs of memory and new forms of co-processing has weakened much of the conventional crypto over the years in the face of brute-force attacks. Similarly, the threat of side-channel attacks (discussed above) offer enough clues that brute force attacks suddenly become viable on conventional hardware on otherwise seemingly secure crypto. Algorithms like DES and RSA512 which were not long ago considered sufficient for the most secure applications, have fallen in the face of Moore's Law.

However, the most existential threat to conventional (and sovereign) cryptography on the horizon is that brought by quantum computing. A quantum computer of sufficient strength using Shor's and Grover's algorithms will defeat virtually all asymmetric, symmetric, and hashing functions. In the case of asymmetric cryptography, the failure of conventional algorithms is complete: RSA and ECC are considered entirely vulnerable to quantum attacks. In the case of symmetric and hashing functions, these algorithms are considered to remain viable (for now) if their lengths are at least doubled. But no one really knows for certain if new mathematical attacks will quickly emerge rendering those vulnerable as well, once we have quantum computers at sufficient scale available for testing.

The arrival date of quantum threats is unknown at this time. The National Academy of Science in the United States says that they expect a quantum computer to reach a useful (aka "cryptographically dangerous") scale in roughly 20 years' time (2038). Some academics working in the field are more pessimistic (or optimistic?): they believe we have a 50-50 shot of seeing a quantum computer strong enough to obliterate conventional cryptography in the next 10 years (2028) . And if you ask the large enterprises like banks and telecoms, who stand to have their businesses made defenseless in front of a quantum-enabled attack, they will tell you their risk tolerance extends about 5 years (2023). For highly regulated industries, where risk appetite is almost zero, the time is now to start thinking about a post-quantum reality.

Cryptographic Agility – a Holistic Definition

True and complete cryptographic agility is the ability to implement, update, change, and remove cryptographic functions from systems and applications on demand, without changing the systems or applications themselves. Cryptographic agility is required across the spectrum of devices, applications, and systems we use today as consumers and business, because cryptography itself is everywhere! See Figure 1.

Cryptographic agility should also include the notion of policy management is another partial form of agility which allows rules to be applied around what type of crypto might be used by an application or system, relative to what is available on the system. For instance, the application might be capable of using weak or deprecated crypto, but the system policy will enforce rules forbidding that crypto from being used. How the policy is enforced is a different matter and beyond the scope of this paper.

Finally, cryptographic abstraction is the process of separating applications from cryptographic libraries with a middleware layer that takes calls for cryptographic functions and directs them to the appropriate cryptographic provider: software, hardware, or firmware. The main use-case for abstraction is to decouple applications from cryptography so that an update to the available crypto does not require the application to be re-compiled, re-installed, or perhaps even re-started. Because the cryptography has been separated from the application and is easily updated or modified, the application achieves a cryptographically agile state.

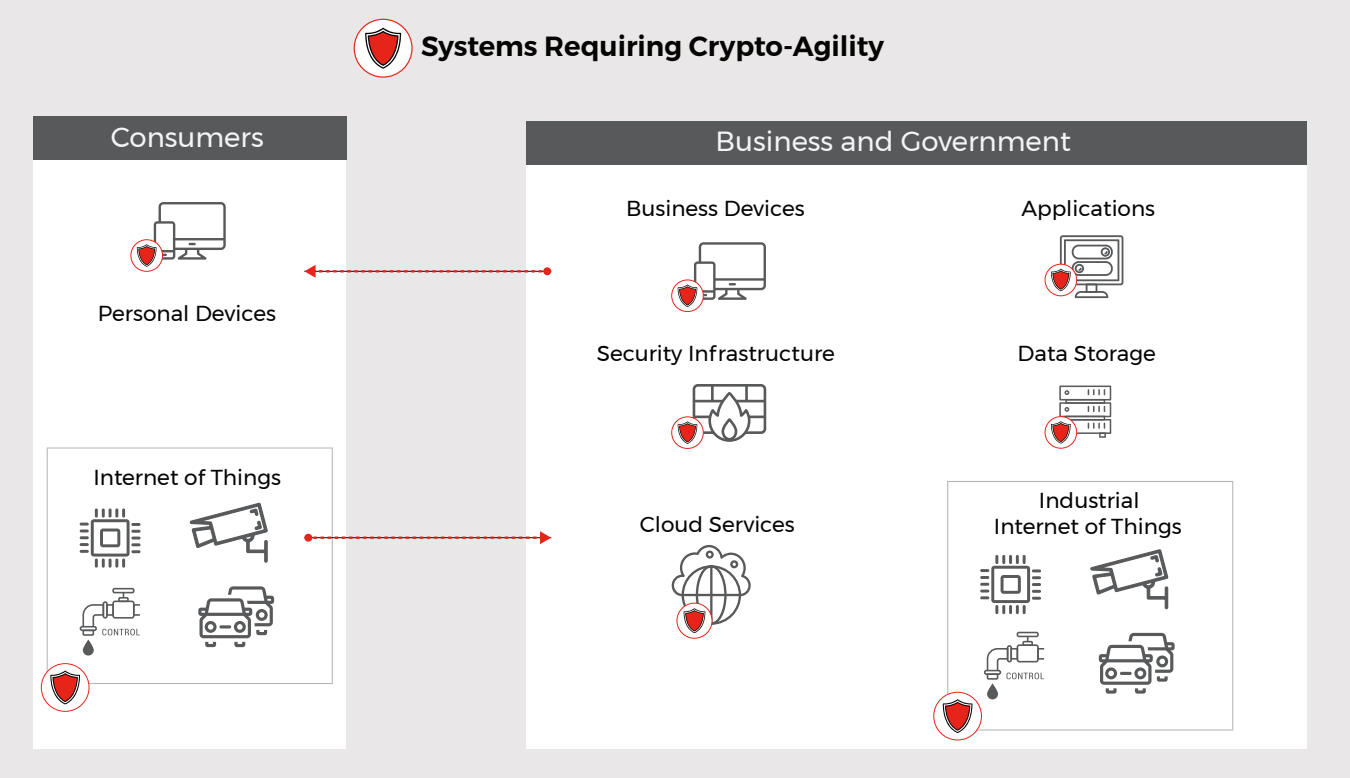

Figure 2: Devices and systems requiring cryptographic agility

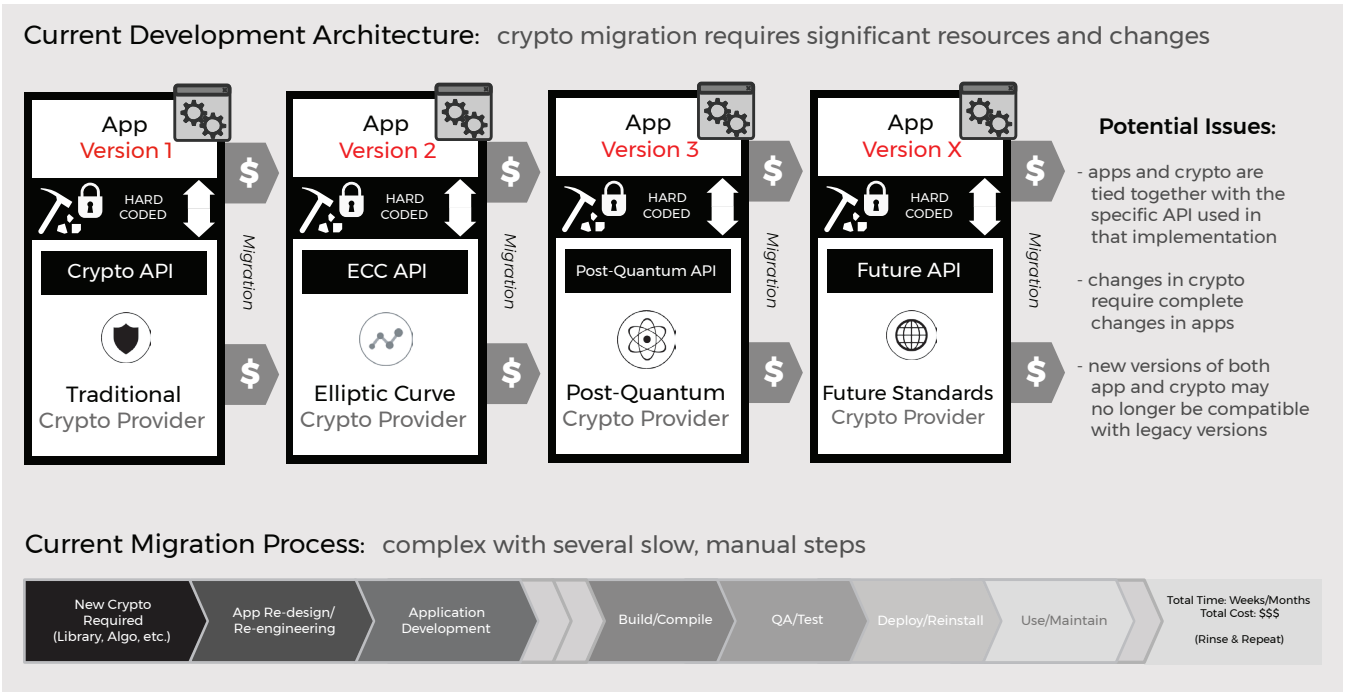

Figure 3: Applications lacking cryptographic agility are difficult to modify

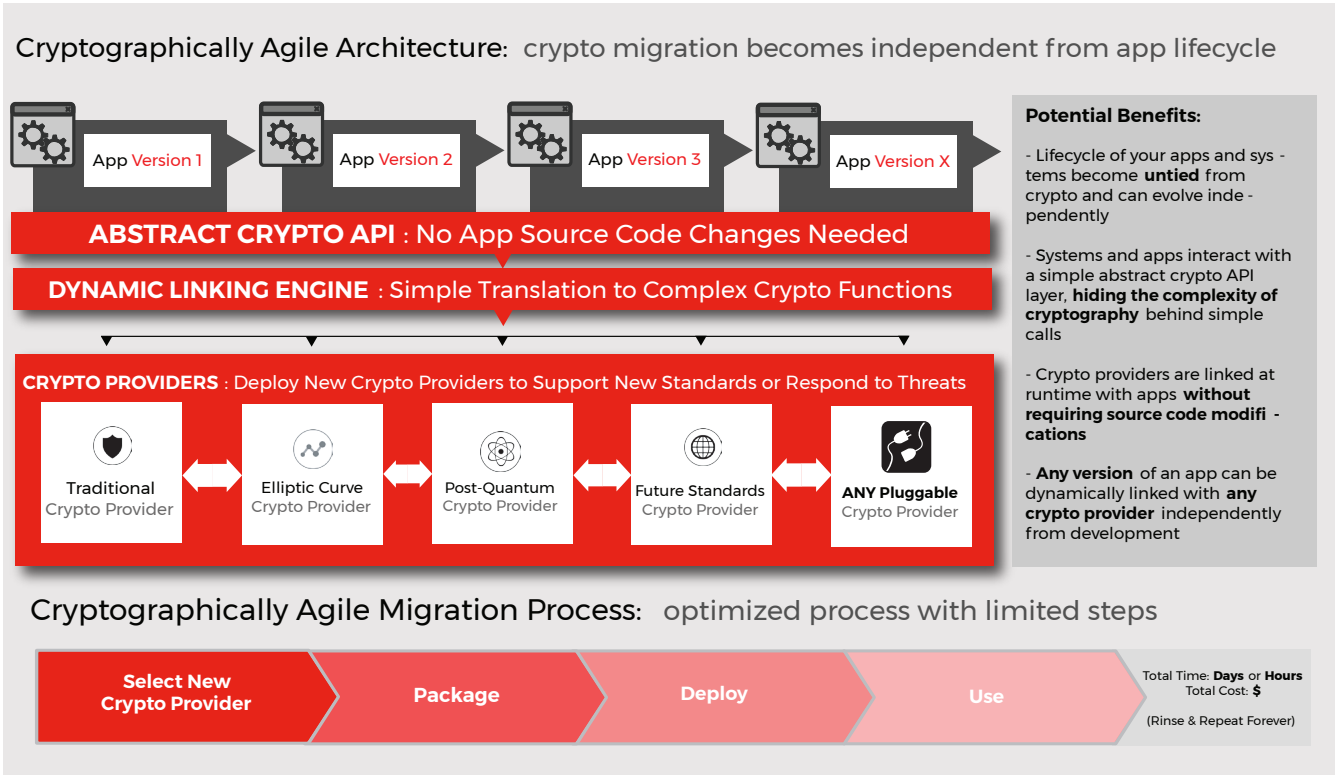

Figure 4: A cryptographic agility architecture makes changes simple and expeditious

Use-Cases for Cryptographic Agility

The following are samples of how and where cryptographic agility may be required in different industries. We have categorized the use-cases into two broad variants: value-added and operational:

A value-added use-case is one that differentiates a product or service. Differentiation can result in the ability to increase price, or results in higher attraction and retention of customers. In either case, the product or service generates more revenue.

An operational use-cases is one that results in savings and therefore higher margins. Savings may be in production efficiency, reduced defects and losses, reduced downtime and outages, and decreased start-up and shutdown frequencies and durations.

Use-Case #1 – Mitigating New Crypto Vulnerabilities

Value-added	Software and Platform Makers: as cryptographic flaws and weakness continue to mount against conventional algorithms, new attacks are discovered, and computers become more powerful, the ability to configure, remove, and update cryptographic functions to respond to risk is seen as a benefit. Service Providers Example: agile certificates for identity management – customers not concerned about rapid and uncontrolled transition from Classic to PQ identities – the certificate will remain valid for the intended lifetime. This will deliver a higher customer confidence in the longevity of the product or service and lead to a more attractive offering to new customers and retention of existing ones.
Operational	Service Providers Example: when a new cryptographic vulnerability is announced as a result of implementation flaws or new attacks, applications and operating systems typically need to be upgraded, patched, re-installed, or flashed with the resulting downtime that entails. Usually this equates to extended periods to implement and long risk exposures with high costs. Cryptographic agility can allow for new cryptography to be implemented by updating a single library or potentially just re-configuring to use a different (not effected) cryptographic provider for the same functions. This allows a service provider to substantially reduce the window of opportunity for an attacker to exploit a new vulnerability and significantly reduces the effort required to migrate to a secure solution. Example – agile certificates for identities (again). The service provider can reduce the potential for massive churn and attrition as the result of new crypto flaws. This also provides a safety value to migrate users in the event of a new crypto attack or a quantum-risk, without expensive re-issuance of identities. The outcome is reduced costs in the event of a need to migrate from classic to post-quantum cryptography (PQC) + avoidance of uncontrolled migrations.

Use-case #2 – Compliance to Local Laws or Standards

Value-added	Financial Services Example: differentiated mobile apps and services based on the ability to offer enhanced, tailored, and customized crypto to applications and clients that want more security – not the status quo of baked-in crypto that can only be changed by re-installing software every time you enter a new region. This delivers increased convenience for customers and a better user-experience by minimizing disruption to consumers if changes are needed. Moving to pre-specification Post Quantum Cryptography should be done immediately ahead of the NIST standardization efforts. The threat of harvest and decrypt risks to both data in-motion and at-rest is real to financial services firms whose entire reputation is based on maintaining the secrecy and confidentiality of their customer information. Software and Platform Examples: auditors are asking questions about how cryptography is managed – not merely used; making agility a decision factor in procurement and support. Being able to demonstrate to auditors that you are using effective and strong cryptography and can pivot to new forms if circumstances dictate can streamline your regulatory compliance efforts around data protection.
Operational	Financial Services Example: as customers roam to different locations, services can follow them and remain compliant with local laws. For instance, a mobile app detects that it has changed jurisdictions based on GPS, carrier, or other localization information, and adjusts cryptography accordingly. Compare this to current options where a customer may need to download a new, country-specific version of an application, or worse: the application no longer works at all because the organization can not meet the compliance obligations of that nation. Cloud and SaaS Provider Example: allow standardized products to be replicated around the world without the need for different versions with different hard-coded cryptography – the cryptography used is simply plug-n-play based on the locality that the data is housed in, or where the customer is located: US crypto in the US, Korean crypto in Korea, Chinese crypto in China. Build your applications and products once, and run them anywhere you wish. All sectors: Cryptographic hybridism allows for both post-quantum safety and compliance. Different forms of hybridism will apply in different localities. Implementing hybridism will allow you to prepare for post-quantum cryptography without committing to a non-compliant or standardized algorithm.

Use-Case #3 – Amortization of Industrial IoT

Industrial IoT (IIoT) is typically defined as connected devices and assets associated with heavy industry or infrastructures. For instance, factory floors, power grids, mass transportation systems, and water systems are all examples of Industrial IoT.

Value-added	***When: Now*** There is an opportunity for IoT device manufacturers to augment their services business with crypto management and compliance services that extend past the time of manufacture. This Industrial IoT Security as a Service will ensure the secure, functional lifetime of devices to the end of its amortization period because crypto risks can be addressed effectively and on the basis of service levels. For a business, risk can be treated internally or transferred to third parties through service agreements - we call this risk transference. A poorly deployed or a mismanaged update to crypto can result in a device becoming "lost": the device may become unavailable, unresponsive, or worse, "bricked". Alternatively, if an update is not deployed in a timely manner, the device may fall prey to a remote attacker who will subvert the device or otherwise take control of it. The only remedy beyond that point will be a physical re-install or physically triggered re-boot back to factory setting. The costs of doing this might be prohibitive, especially with devices in remote areas.
Operational	***When: Now*** By allowing the movement to pre-specification PQC or sovereign algorithms now, the threat to business cases posed by the need to do a rip and replace later to address flawed, weak, or outdated crypto (or the addition of new sovereign requirements) is eliminated. This also allows the standardization of products that can be sold and deployed worldwide without the need to build and support unique localized versions with different cryptography based on local needs. This also delivers better regulatory compliance by ensuring any data collected by devices is always encrypted using the most recent and strong crypto – both in-motion and at-rest.

Use-case #4 – Platform Design

Platforms are things that fly, float, or roll. They are the airplanes, boats, cars, trucks, and trains we have all around us, which are for all intents and purposes now moving data-centers. These platforms are, or are rapidly becoming, highly interconnected, supporting a variety of networks for connections to other platforms: to IIoT systems in ports, stations, and homes, and to the Internet generally for onboard entertainment, navigation, and service-support functions from third party providers. Cryptography is used widely to support both the identity and confidentiality of associated with these platforms and networks.

Platforms themselves can contain many networks, each supporting different functions and control systems. On each of these networks there may be different nodes and devices, which interoperate and communicate with each other as well as with other devices on other networks. For example, engine monitoring and diagnostic systems will necessarily communicate with human-interface dashboard systems. Safety systems monitoring airbags and crash sensors will have access to cellular communications to alert first responders to impacts and other events likely to require assistance for passengers. Anti-theft systems often have cellular connections to allow service arms of manufacturers to remotely disable a vehicle if requested by law enforcement.

Platforms by their very nature are designed to move in some fashion. In many cases they will cross international borders, moving from one regulatory environment to another. They might do this as a matter of day-to-day business, or they may be built in one jurisdiction, but sold for use in a different jurisdiction – never to return to its origin. Additionally, platforms have long lifespans – more like industrial IoT than enterprise IT. Most platforms will have planned lifespans and spare parts to support 20 years of operation; however, in reality, some platforms may spend twice that amount of time in service.

Value-added	***When: Now*** There is an opportunity for IoT device manufacturers to augment their services business with crypto management and compliance services that extend past the time of manufacture. This Industrial IoT Security as a Service will ensure the secure, functional lifetime of devices to the end of its amortization period because crypto risks can be addressed effectively and on the basis of service levels. For a business, risk can be treated internally or transferred to third parties through service agreements - we call this risk transference. A poorly deployed or a mismanaged update to crypto can result in a device becoming "lost": the device may become unavailable, unresponsive, or worse, "bricked". Alternatively, if an update is not deployed in a timely manner, the device may fall prey to a remote attacker who will subvert the device or otherwise take control of it. The only remedy beyond that point will be a physical re-install or physically triggered re-boot back to factory setting. The costs of doing this might be prohibitive, especially with devices in remote areas.
Operational	***When: Now*** By allowing the movement to pre-specification PQC or sovereign algorithms now, the threat to business cases posed by the need to do a rip and replace later to address flawed, weak, or outdated crypto (or the addition of new sovereign requirements) is eliminated. This also allows the standardization of products that can be sold and deployed worldwide without the need to build and support unique localized versions with different cryptography based on local needs. This also delivers better regulatory compliance by ensuring any data collected by devices is always encrypted using the most recent and strong crypto – both in-motion and at-rest.

Use-Case #5 – Cloud Services: Build Once, Run Anywhere

A significant part of the business efficiency of cloud services is contained in the ability to run the same software in many different locations, expanding and contracting on demand, gaining economies of scale, which benefits both the cloud provider and the customer. As regulations and standards around cryptography both fragments and evolves, cloud service providers (CSP) will encounter complications associated with services from highly centralized locations based on homogenous software platforms. For instance, the end of Safe Harbor has meant that CSPs like Google, Amazon, and Microsoft have had to establish more and more local presences, and have had to adjust local configurations and policies to meet the requirements of local laws and regulations. Cryptographic agility offers important opportunities to regain efficiencies and potentially capture new forms of revenue in the face of the changing nature of the cloud services business.

Value-added	Compliance Management Services targeting multi-national service providers with complex inter-jurisdictional obligations. In most cloud services, a baseline of functions is provided, including security functions. A value-added opportunity exists to offer enhanced management functions which include crypto agility, as well as automated agility. For instance, decrypting and re-encrypting data as if flows from one domain of control to another using the appropriate algorithms. Hybrid Encryption is a novel form of cryptography which has the ability to meet multiple requirements at once and may also be offered on an upsell basis. Hybrid encryption can mean different things in different applications; however, one use-case is where data is encrypted twice or even more to achieve regulatory compliance and in some cases quantum-safety for data storage. Hybridism is essentially mixing different algorithms with different properties so that the custodians can claim combined properties. In one case this may be that a prescribed algorithm is used, in another case it may be that a customer wants a quantum safe algorithm to protect against long term decryption attacks by a state-sponsored adversary. In either case, no single algorithm is likely to meet both requirements, while hybridism may meet their needs. Hybridism can be applied to both data and rest and data in transit – offering multiple opportunities for hybrid-service bundles and options.
Operational	Overcoming trade barriers. Even more so than Industrial IoT or Platforms, cloud services may be vulnerable to trade barriers built upon cryptography as sovereign crypto becomes more and more prevalent, and local requirements to support different crypto take effect. Looking at it from a different perspective, customer satisfaction is a major form of operational efficiency. Giving customers the ability to configure and migrate data protections from one form of cryptography to another from an administrative dashboard or interface will be a prized and powerful feature for multi-nationals and even small businesses doing business across international borders. Regulatory reporting and auditing related to cryptography is a rapidly growing cost for cloud service providers (and enterprises of all sorts). Cryptography is typically unmanaged and often its location in libraries, binaries, and Java files is poorly understood and definitely not comprehensive. As regulators and customers alike demand more control of the crypto being used in service delivery, and also demand proof that requirements have been met, costs will inflate rapidly. Cryptographic agility and the reporting and management infrastructure around it will offer the ability to automate both regulatory reporting and audit.

Use-case #6 – Interoperability

To put it succinctly: agility enables more fluid interoperability. One of the main reasons so much old, weak, and deprecated cryptography continues to persist is because guaranteeing interoperability across the entire userbase means that bad crypto can never be removed from general libraries.

Value-added	Development houses can guarantee cryptographic interoperability indefinitely. By embedding a cryptographically agile middleware layer inside applications provided to customers, companies who build applications or services for other organization will be able to add a new upsell layer or service-driven source of revenue for those customers. By guaranteeing their applications will work in any region, and can be updated quickly in the case of a new threat or vulnerability, developers can drive incremental revenue from their existing customer base and attract new customers away from competitors.
Operational	Policy enforcement becomes simple for organizations. Using a cryptographic agility layer to enforce allowed versus prohibited algorithms can prevent the inadvertent use of bad cryptography. Because the application with agility no longer needs to call specific algorithms, it can just request functions like "key exchange" or "stream cipher" (among others) and let the agility layer filter out the deprecated algorithms. Additionally, if two parties to a transaction are required to use specific or sovereign cryptography, then agility makes it easier for them to use it without having to go back to either their in-house development teams or the vendors to request updates or modifications.

Requirements for Agility

Based on the risks and use-cases associated with cryto-agility, the following broad requirements define crypto agility as a concept and functional target:

1. Real-time; the ability to install/implement crypto without re-coding or even re-booting applications and systems
2. Heterogenous; algorithms are available by a mix of software, hardware accelerated and HSM-based crypto providers
    a) Classic and post-quantum use and adoption is not a factor of the access – it is a about whether the application itself is able to support the "shape" of different algorithms: key sizes and processing overheads
    b) Provider-neutral and able to adapt any form of crypto primitive from any source – specifically to support sovereign cryptography but currently un-conceived algorithms.
3. Policy-aware:
    a) Administrators set policies about which primitives and algorithms may be accessed by applications
    b) Requires careful engineering-policy when substituting classic for PQC
    c) Policy interface must itself be highly secure because it is an attack point.
4. Automated, centralized and / or peer to peer provisioning. Crypto agility will be most valuable when it can be employed across large populations of devices in very short periods of time or automatically according to attributes like time, place and useage context.
5. Scales from IoT to Cloud: abstraction must be deployable across a wide range of platform. Java-based agility would be limited.
6. Application Interoperable – ideally, agility API calls are standardized so that application makers do not need to choose an agility vendor (argues for Open Source)

Conclusion: How to Fix the Problems Facing Cryptography

Addressing these crypto-risks requires first the acknowledgement that cryptography needs to become something that is changeable, not static. Statically integrated cryptography has no ability to pivot away from the risks discussed above, which means the applications and systems relying on such cryptography become vulnerable and stay vulnerable.

The best answer is to make cryptography agile – dynamically adjustable to the risks presenting themselves. While it is possible to continue with the convention of hard-coding cryptography into applications and services, this will add cost and increase vulnerabilities. In some cases, the vulnerability will not only be to attackers, but to regulators.

Cryptographic agility is a best practice, and the standard against which auditors will render opinions about cyber security. Expect to see agility becoming part of International cyber standards first and eventually laws and regulations.

About InfoSec Global

Infosec Global provides sustainable data protection for a digital world. The company delivers a next generation enterprise grade solution that provides real-time life-cycle management of the cryptography and digital identities for critical systems. The AgileSec Platform manages the entire digital and cryptographic life-cycle from the discovery of threats and vulnerabilities to the updates and fixes of cryptography, keys and certificates. ISG helps governments and enterprises achieve trust through compliance to cryptographic regulations, worldwide.

To learn more, visit **www.infosecglobal.com**

Additional articles and resources on crypto agility:

Better Safe Than Sorry: Preparing for Crypto-Agility
By Mark Horvath and David Mahdi, Gartner
http://bit.ly/gartneragility

Cryptographic Agility Animated Demonstration – watch the video:
http://bit.ly/cryptoagilityvideo

What does Crypto Agility mean for Post-Quantum Cryptography Solutions?
By Dr. Basil Hess, ISG Research Team
http://bit.ly/ISGpostquantumagility

Crypto Agility is a Must-Have for Data Encryption Standards
By Nagy Moustafa, CEO of ISG and Dr. Vladimir Soukharev, ISG Research Team
http://bit.ly/ISGwhyagility

Cryptographic Lifecycle Management, A New Market Category is Emerging
By Claire Trimble, CMO, ISG
http://bit.ly/agilitynewmarket

Presentation on Cryptographic Lifecycle Management, PrimeKey Tech Days 2018
By Dr. Tomislav Nad, ISG Research Team
http://bit.ly/ISGprimekeyvideo

INFOSEC GLOBAL
FEDERAL

SAN FRANCISCO
750 Battery St.
San Francisco, CA 94113

TORONTO
2225 Sheppard Avenue East
Suite 1402, Toronto, ON
M2J 5C2 Canada

ZÜRICH
Hardturmstrasse 103
8005, Zürich
Switzerland