Manu Fontaine
Founder and CEO
Hushmesh Inc.
A Public Benefit Corporation

To whom it may concern:

Recent advances in Trusted and Confidential Computing (2020) have enabled a new approach to cross-domain cybersecurity, with groundbreaking benefits for secure supply chain automation. This new approach solves "universal authenticity" for things and people by enabling cryptographic "chains of data custody" at global scale.

Today's supply chain systems are built on relational databases. Identifiers (for things and people) and related data are all domain-centric, and all bindings are merely relational. Insiders and attackers (with sufficiently escalated privileges) can tamper with them with potentially devastating consequences for any system relying on them. This current state precludes "universal authenticity", i.e., the global assurance of provenance and integrity.

The new approach contemplates the use of global cryptographic identifiers for all real-world entities. Called "Stem IDs", these identifiers are 256-bit truly random numbers generated and exclusively managed within trusted and confidential computing environments. By design, Stem IDs are both identifiers and cryptographic keys, which inherently solves the entity-key binding.

This elemental construct enables the cryptographic derivation and binding of aliases, keys, encrypted data, signed software agents, attested hardware and cryptographic routing for any real-world entity. The new approach in turn enables the automation of end-to-end cryptography between any such entities to create globally assured "chains of data custody".

Cryptographically-bound aliases can then be expressed as QR codes on individual items of any product in any supply chain. These cryptographic codes can be resolved with global assurance to their original Stem IDs and all that is bound to them. This secures all supply chain data in a global, cross-domain fashion that was simply not possible before. The resulting attack surface is as small as can be, as all bindings are cryptographic, all data are encrypted, all software is signed, and all hardware is attested.

We propose that NIST consider this approach as a new "Cryptographic Name System" for everything and everyone. Today's domain-centric approaches to naming and relational databinding inherently preclude global supply-chain security. Only by closing domain-centric vulnerabilities will we be able to securely and seamlessly automate global supply chains.

As a Public Benefit startup, we would love to present our work to NIST and anyone else who should see it. We look forward to hearing from you.

Best Regards,
Manu Fontaine

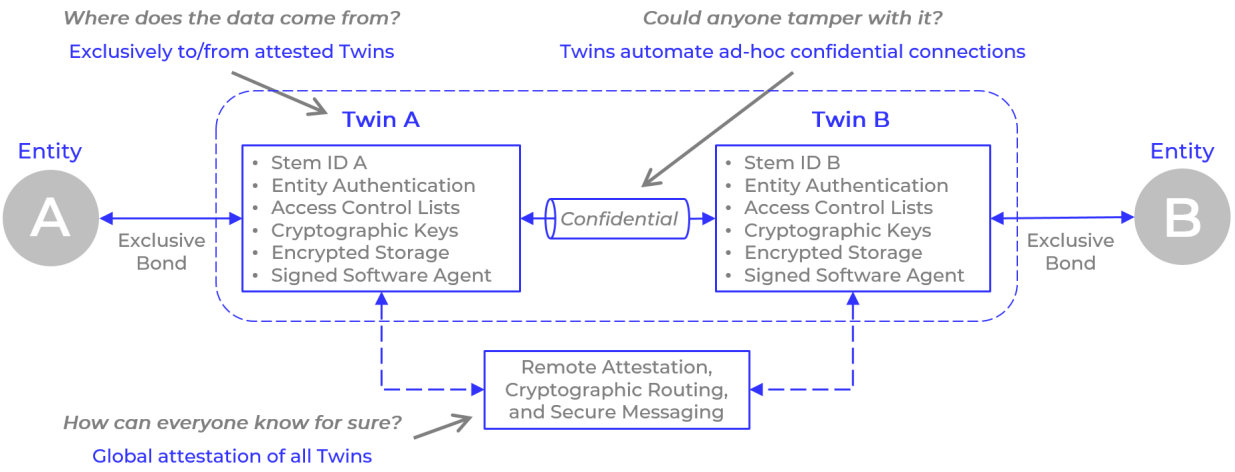
Solving Universal Authenticity for Everything and Everyone

Solution Overview - April 2022

The internet has a big problem. To this day, it has remained impossible for any two real-world entities to seamlessly transact or exchange data with global assurance of authenticity and confidentiality. Uncertainty about origin, fidelity and authority is a root-cause of cyber attacks and fraud, a fast-growing trillion-dollar problem, impacting billions of people, across all industries and communities worldwide.

Everyone agrees that ubiquitous, end-to-end cryptography is the solution. But cryptography is unforgiving, and humans are unreliable. Today's cryptographic approaches rely on people's skills, attention to details, and good behavior, which makes them fragile and vulnerable as a result. Removing humans from all cryptographic operations is hence essential to achieving global assurance of data provenance and integrity. All key management and cryptographic primitives must be automated at the edge in a way that can be remotely verified and globally attested.

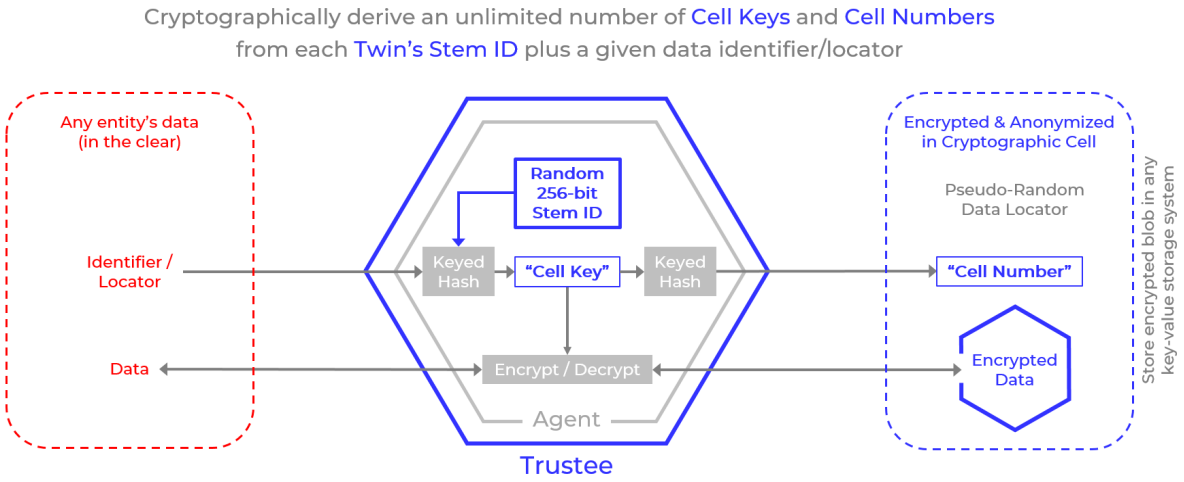
The solution is to bind each and every real-world entity (people, orgs, apps, files, things…) to its own unique and unclonable *Cryptographic Twin*. Each Twin exclusively represents its real-world entity and acts on its behalf in cyberspace. Cryptographic Twins run on *Trustees:* trusted and confidential computing environments that enable remote attestation of their integrity. Trustees provide global assurance of the quality and confidentiality of all cryptographic material and primitives managed by the Twins. Trustees are powered by Microsoft's Azure Sphere and Azure Confidential Computing.



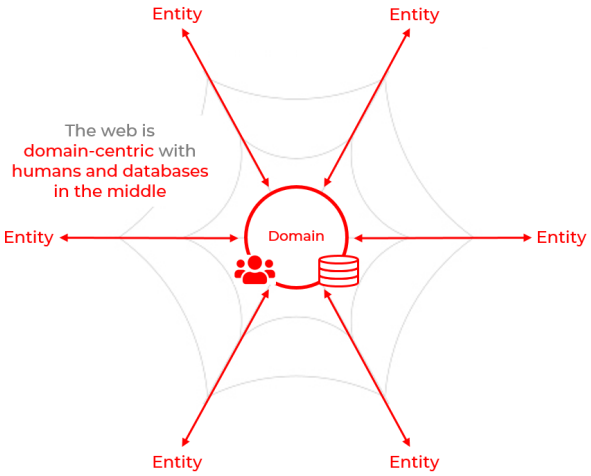
Each Twin is "born" from a secret, truly random 256-bit *Stem ID*, generated by a high-quality true random number generator, and protected at all times within trusted computing silicon. Thanks to its true random nature over an enormous range of possible values, a Stem ID is *simultaneously* a Twin's definitive private identifier and its main 256-bit AES key.

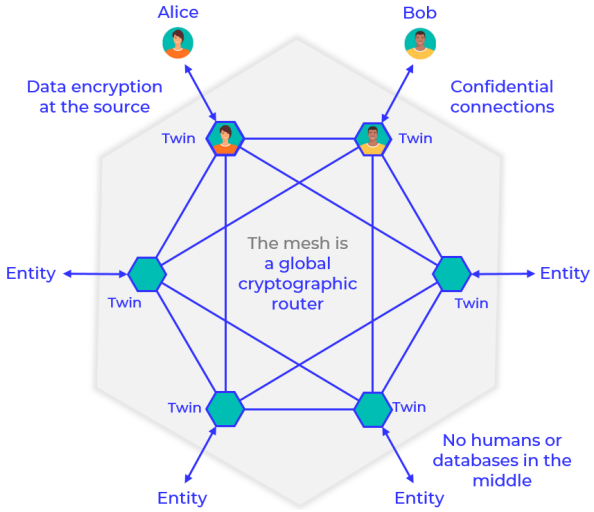
Leveraging the strong cryptographic quality of its Stem ID, each Twin can derive an unlimited number of private *Cryptographic Cells*, and use the Stem ID for exclusive and secure access to all its daughter Cells. A Cryptographic Cell is a virtual unit of encrypted storage defined by a unique *Cell Key* and unique *Cell Number*. A Twin derives Cell Keys and Cell Numbers from its private Stem ID through a series of one-way hashes, with each daughter Cell being specific to a different application context. Each Twin can then encrypt the entity's data for that application with the corresponding Cell Key, and store the encrypted data *in any data store* at a location pointed to by the corresponding Cell Number.

This universal and recursive construct guarantees the cryptographic binding of every Cell and of all encrypted data in each Cell back to the Twin's Stem ID. In turn, this provides global assurance of the integrity of each Twin as an authentic cryptographic representation of its corresponding entity.



Trustees run signed software Agents which enable Twins to transact with one another. The exchange of keys and establishment of confidential connections can be fully automated between any two Twins, as all Twins are remotely attested as authentic and cryptographically healthy through the Azure Sphere and Confidential Computing attestation services. This approach gives rise to a cryptographically defined network topology we call the *Mesh*. Integral to the Mesh are remote attestation, durability monitoring, orchestration services (such as cryptographic routing and secure messaging), distributed blob storage, and a unique distributed peer-to-peer backup service.





We now have the tantalizing opportunity to bind every real-world entity to its own Cryptographic Twin, with every Twin securely addressable by any other Twin. The Mesh is a global cryptographic "switch board" that automates end-to-end cryptographic security between any two real-world entities, which solves seamless authenticity and confidentiality for all ad-hoc data exchanges and transactions.

Benefits of the Mesh

- Entity-centric automated key management
- Entity-centric data encryption
- Anonymized encrypted data storage
- Non-replayable data claims by entities
- Automated secure pair-wise encryption
- Ad-hoc, secure IoT connections
- Zero-knowledge proofs
- Entity cryptographic records / auditability