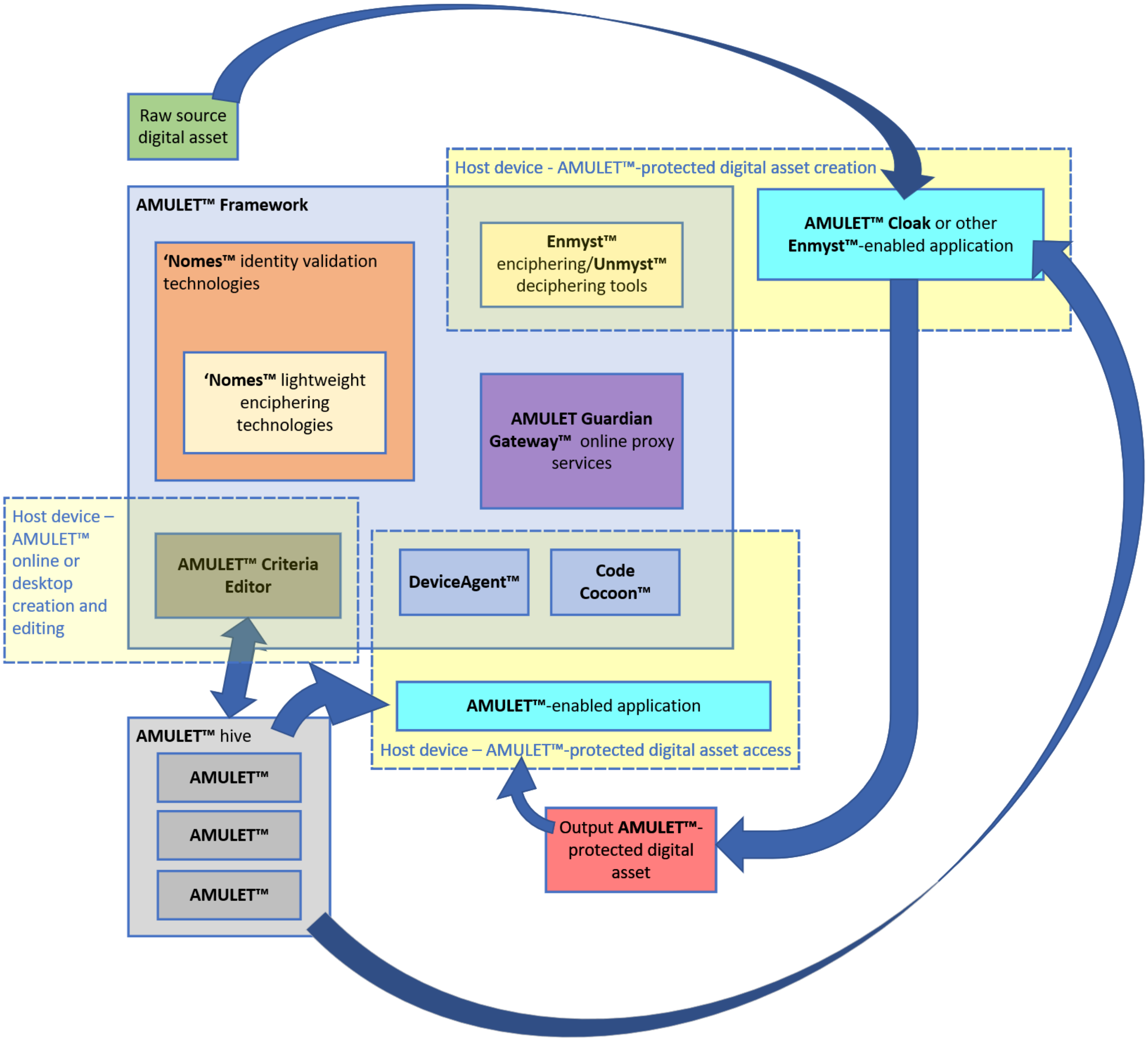
Raw source digital asset
Host device - AMULET™-protected digital asset creation
AMULET™ Framework
Enmyst™ enciphering/Unmyst™ deciphering tools
AMULET™ Cloak or other Enmyst™-enabled application
'Nomes™ identity validation technologies
'Nomes™ lightweight enciphering technologies
AMULET Guardian Gateway™ online proxy services
Host device – AMULET™ online or desktop creation and editing
AMULET™ Criteria Editor
DeviceAgent™
Code Cocoon™
AMULET™-enabled application
Host device – AMULET™-protected digital asset access
AMULET™ hive
AMULET™
AMULET™
AMULET™
Output AMULET™-protected digital asset

The AMULET™ Framework technology map

Version 1.1

F. Scott Deaver
CTO
September 24, 2020

Table of contents

[The technologies described here are exclusive and proprietary to F. Scott Deaver and Certitude Digital, Inc. They are represented by issued patents, patents pending, copyrights, trademarks and underlying trade secrets protected by intellectual property law. We offer them here in the spirit of transparency and education as a public service to enhance awareness with the intention to help prevent crime and abuse, and with the expectation that our rights will be respected. We intend to enforce those rights as required.]

The AMULET™ Framework

"The AMULET™ Framework" is the term we use to refer to the totality of components and services that together comprise Certitude Digital's complete solution to all aspects of the cybersecurity problem domain.

In older documentation, we often used the term "AMULET™ framework" to reference that component where we do all of the work on an individual device to bring together the various pieces - one or more AMULET™s themselves, the AMULET™-protected digital asset, and the data accumulated about the device's environment need to answer the questions contained in the protective AMULET™s' criteria - to determine whether access should be granted under the current circumstances, and if so, to process the access request.

In hindsight, people coming from other environments found ***that*** use of the word "framework" confusing, believing that "framework" should instead describe the overarching scaffolding over the entire technology, and we decided they were absolutely right. Therefore, we have begun referring to the on-device workhorse component as the "AMULET™ DeviceAgent" instead, and use "AMULET™ Framework" now to refer to the entire collection of components and services that comprise the system as a whole. These are the terms as we will use them consistently going forward, and we get the time and opportunity, we will correct some of that older documentation.

The AMULET™ Framework, then is the governance over the AMULET™ system as a whole, and this document describes the relationships between the components of which the system is comprised (and briefly, the components themselves). I have appended at the end a list of some of products, services, and systems that we are in the process of designing, have demonstrated, or are actively building.

Enmyst™

Before I get into the technology map itself, though, I wanted to address one more bit of leftover nomenclature business. Our very-carefully-architected and nurtured enciphering technologies have matured and grown beyond anything we could have ever imagined, in scope, in power, and in potential. Perhaps because in the early days more than twelve years ago, our enciphering was primarily a clever re-purposing of existing standardized protocols mixed with some devious layering and intertwining, we never bothered to give it a name, clumsily referring to it first as encryption, and when that became inadequate, enciphering, to which we prepended long and varied set of adjectives and adverbs (actually, "AMULET™" is nothing more than an acronym for one of those long strings).

Now, we have our own enciphering patents pending, we regularly use proprietary techniques that bend the limits of what is possible in terms of both efficiency and complexity, and we expand our enciphering capabilities daily. It is high time we gave this stuff a name, and we have decided to use as the root "Enmyst" (as either a verb or a noun). A list of all of the forms we will be using includes: "Enmyst™" (root), "Enmysted™", "Enmystify™", "Enmystified™", "Enmystifying™", "Enmysting™", "Unmyst™", "Unmysted", "Unmystify™", "Unmystified™", and "Unmystifying™". We have registered "Enmyst.com" as a domain name and intend to eventually point that to a web page describing and promoting the technology, and depending upon demand, offering it in one or more forms as a standalone product outside its primary role supporting AMULET™s.

The AMULET™ Framework technology map

With that, on with our technology map…

Components

1. The raw unprotected digital asset

This is the source material the content provider wants to secure.

2. Enmyst™ technologies

These encipher AMULET™ itself, as well as the resulting AMULET™-protected enciphered digital asset.

2.a. "Kerckhoffs' Complement™"

The very basic elements of battlefield encryption were described in "Kerckhoffs' Principle", laid out by Auguste Kerckhoffs in 1883. We have honored those principles by applying his name to our patent-pending and trade-secret collection of modern improvements upon cryptography, adapted for the digital realm. Some of the manifestations of those improvements are listed below.

2.a.i. Multilayered

A digital asset is enciphered in one to *n* randomly-assigned layers, where the number of ;ayers as well as the enciphering method used for each layer are determined by a random number generator at the time of invocation.

2.a.ii. Nested

Each layer contains one to *n* randomly-assigned segments per layer - a layer's segments may be mixed, comprised of various types of encryption or enciphering, or a given segment not be enciphered at all. The number of segments and the enciphering method used for each segment are determined by a random number generator at the time of invocation.

2.a.iii. Interleaved

Depending upon the interpretation of the numbers emitted by a random number generator, a layer's bytes may be intertwined pre- or post-enciphering in various patterns for segments randomly sized independently of enciphering segments. The bytes of one layer may be interleaved with the bytes of another layer before or after the enciphering of either or both layers.

2.a.iv. One non-trivial segment uses standard publish encryption methods

At least one non-trivial segment of at least one layer will be enciphered with one of several possible standard published encryption methods that comply with Kerckhoffs' requirement for the encryption methodology to be publicly known. Other segments, regardless of layer, may use a non-standard encryption method, simple byte substitution or X-OR'ing, or no enciphering at all. When properly implemented using interleaving, the logical benefits of having at least one non-trivial-segment in at least one potentially multi-segment layer of a potentially multilayer enciphering process using publicly-known encryption methods naturally flow to all other segments and layers - layered encryption is actually as strong as its strongest link (where in our case, a segment of a layer is a link).

2.a.v. Keyless

The information understood by system components to be available from the AMULET™ itself as well as the encoding that links the AMULET™ to the AMULET™-protected digital asset is sufficient to uniquely and unequivocally protect the contents of that digital asset. Think of the AMULET™ and the links to it within the protected AMULET™-protected digital asset as one giant unique passkey.

2.a.vi. Bytecode produced by the Enmyst™ process is both size- and byte-content variant

No two enciphering passes on the same raw digital asset produce the same bytecode results or output file size, even when performed in sequence on the same device with all inputs identical.

2.a.vii. Version-mapped internal identifiers

Identifiers for the variety of nesting techniques, interleaving patterns, enciphering technologies, layering schemes, and other data-driven elements, as well as the mappings of any re-used identifiers and the specific entities they represent, are changed between each of the AMULET™ versions issued.

3. 'Nomes™ identity validation technologies

This component identifies and validates the parties when the party must be known to satisfy an AMULET™'s criteria.

3.a. 'Nomes™ enciphering technologies

'Nomes™ technologies have their own lightweight encryption methods based on adding unique identity data to standard enciphering keys, suitable for less-capable devices.

4. AMULET™

An AMULET is a collection of questions having yes or no answers posed by the content provider or owner of a digital asset that are asked of the host device's surrounding digital environment when a request is made to access that digital asset. If all of the questions asked of the environment (as well as any questions posed by any other AMULET associated with the digital asset) all result is "yes" answers, access is granted and the digital asset is temporarily Unmysted™ into a secure Code Cocoon™ isolation area for streaming to the requesting authorized app or service.

4.a. Criteria are defined by the owner/creator of a raw unprotected digital asset

The content provider selects and modifies the questions to be asked in an AMULET™'s criteria through an AMULET™ Editor prior to use.

4.b. The AMULET™ and the AMULET™-protected digital asset are stored separately

Enciphered encoding understandable to the DeviceAgent™ and AMULET™-enabled apps like AMULET Cloak™ provides links to required AMULET™s, and are embedded into each AMULET™-protected digital asset. The unique byte-wise content of portions of these links along with unique byte-wise content of portions of the digital asset as well as unique byte-wise contents of portions of the AMULET™(s) themselves provide any specialized seeding necessary to internal Enmyst™ operations for enciphering or deciphering, as appropriate. At the time a request for access to an AMULET™-protected digital asset is invoked, all of the AMULET™s linked to the digital asset as well as the protected digital asset itself must be within reach of the DeviceAgent™, though they need not be stored together. Generally speaking, an application will pre-register the AMULET™s associated with the protected digital assets it is interested in, so that the DeviceAgent™ can pre-determine the answers to environmental questions before access to the digital asset is requested.

5. DeviceAgent™

This is the component, one to each device and usually loaded at the startup of the device, which does all of the heavy lifting when it comes to determining whether access is to be permitted to an AMULET™-protected digital asset. There are two forms of the DeviceAgent™ - in the standard form, the DeviceAgent™ ensures version currency of the DeviceAgent™ itself as well as any AMULETs it comes in contact with when online, gathers device environment information in the background that may be needed to satisfy AMULET™ criteria, prequalifies AMULET™ criteria for AMULET™s that have been registered with it for impending use. It then reacts to protected digital asset access requests from AMULET™-enabled applications and services, verifying that the current device environment satisfies all of the criteria in AMULET™s associated with the digital asset. If so, digital asset is temporarily Unmysted™ into a secure Code Cocoon™ isolation area, from which it is then streamed to the requesting authorized app or service in segments on a time-leased basis.

In the AMULET Guardian Gateway™-dependent form of the DeviceAgent™, intended for device with slower CPUs, less memory, less storage capacity, or multi-tasking limitations, the DeviceAgent™ collects the device's environment as before, but when an AMULET™-protected digital asset access request arrives, the environment and the request are instead shipped to an AMULET Guardian Gateway™ server via 'Nomes™ lightweight user-identity certified enciphering. The AMULET Guardian Gateway™ server analyzes the AMULET™s associated with the protected digital asset against the enciphered environment data shipped up, and if appropriate Unmysts™ the digital asset into its own secure Code Cocoon™ isolation area, streaming the Unmysted™ results back to the original requesting AMULET™-enabled application or service on the device on a time-leased basis using 'Nomes™ lightweight enciphering.

6. Code Cocoon™

This component provides a safe isolation environment to do the work of Unmysting™ the protected digital asset where no external process can watch, and where any bread crumbs left behind can be cleaned up. After Unmysting™, the deciphered result is streamed out in segments to an authorized AMULET™-enabled application on a short-term timed lease, after which everything is permanently destroyed. Code Cocoon™s come in two flavors - the default is a proprietary-format RAM drive. The digital asset content provider or owner can also, within the AMULET™ criteria, specify the use of a proprietary virtula machine (the same as as used in the Hackless Harbor™ and OphGrid™ applications), and they can select special enhanced security options and other behaviors to be performed on or by the digital asset within the context of a Code Cocoon. In this manner, the output of the Unmysting™ process becomes the results of a hidden function performed by the digital asset rather than the deciphered digital asset itself (and you thought we weren't clever!). When operations are concluded at the end of the time lease (or the requesting app has shut down), the memory area of the Code Cocoon™ (irrespective of the type) is wiped clean and if not permitted for re-use (per AMULET™ Framework system settings), is destroyed.

7. The Guardian Gateway™ online proxy server

This server simulates a requesting device's environment on behalf of the requestor for the purpose of temporarily Unmysting™ an AMULET™-protected digital asset, allowing the DeviceAgent™ a neutral place to do its work, using lighter-weight certified-user 'Nomes™ encryption to ferry sensitive data and results sets back and forth. Rather than use its own device environment to test AMULET™ criteria satisfaction, the Guardian Gateway server uses the hashed and enciphered environment capture sent it by the DeviceAgent™ on the device requesting services.

8. The AMULET™ criteria editor

This editor is the tool that the content provider or owner of a digital asset uses to create and describe one or more AMULET™s to protect their digital asset. AMULET™s are comprised of a series of questions that can be answered yes or no by the digital environment around a hosting device when a request for access is made, along with general security parameters, Code Cocoon custom configurations, AMULET Decloak™ allowance, and notification settings. Yes/no questions that the host device's surrounding digital environment can answer include things like "Is a certain user logged on to the device?", or "Does the user's account have a certain characteristic (like ActiveDirectory group membership)?", or "Is the GPS location of the device within or outside certain coordinates?", or "Is the current time of day within certain limits?", or "Is a specific file or folder available/not available on the device?", or "Do the current contents at a certain location of a given web page accessible from the device match a given range of values?". There are tens of thousands of questions that can be asked, and each provided their own set of match qualifiers, making the range of security options both limitless and unpredictable, very helpful in frustrating hackers.

The output of the editor is an AMULET™ in the form of enciphered content expressed as a unique entry in an XML file known as an "AMULET™ hive". AMULET™ hives are the specific property of registered users in the AMULET™ Framework, and each user's AMULET™s are deposited into that user's designated AMULET™ hive (a user can have several hives).

The content provider or owner of the digital asset links one or more AMULETs™ from the hive to the digital asset and Enmysts™ the digital asset using any AMULET™-enabled app or service, or the AMULET Cloak™ stand-alone app (note that the AMULET™ and the protected digital asset are merely linked by code embedded into the protected digital asset, but remain physically independent - because of this, a digital asset can be protected by several AMULET™s or conversely, one AMULET™ could protect several digital assets or portions thereof).

Trimmed-down copies of the user's master hive containing just the required AMULET™s for a given digital asset are made available online via download, by direct transmission, or by re-use to an intended consumer of that digital asset. The intended consumer can automatically or manually dock the hive into the host device DeviceAgent™'s hive docking area, or otherwise make it available on the Internet or the local file system so that the DeviceAgent™ can find it when an access request is made.

9. AMULET™-enabled application or service

Unmysting™ operations are performed only at the behest of an AMULET™-enabled applications or service. This may be Certitude-Digital-provided application like AMULET Cloak™, AMUmail™, or AMUsourcery™, or it may be a third-party vendor's application or service accessing the AMULET™ Framework through a licensed Software Development Kit (SDK) or Application Programming Interface (API) library. As part of its license agreement, the third-party application vendor has agreed, subject to periodic audit and severe contractual penalties, never to hang on to, copy, re-use, or otherwise persist in any form the content streamed to the application or service by the Code Cocoon™ in response to a protected digital asset access request. The only permitted exception to this rule is via the use of the heavily-self-defensed AMULET Cloak™ application as provided by Certitude Digital. Each and every AMULET™ associated with a given AMULET™-protected digital asset must expressly give permission in their AMULET™ criteria for the use of AMULET Cloak™ in order for the AMULET Cloak™ application to function.

Applications make their Unmysting™ request though a set of licensed API calls (included in the SDK) which can download, dock, and pre-register AMULET™s (if necessary), download (if necessary) one or more protected digital assets, and of course Unmyst™ the digital asset into a Code Cocoon™ and finally access the deciphered content streamed back to the app from the Code Cocoon™.

10. The AMULET™-protected digital asset

AMULET™-enabled apps or services like AMULET Cloak™ bind the raw source digital asset content provider or owner's choice of one or more AMULET™s to the digital asset as embedded links, and then Enmyst™ and output the protected digital asset. The original raw digital asset is disposed of, and the digital asset never appears again in any persistent storage or memory as anything but an AMULET™-protected digital asset

Exemplar prototype products and services created from AMULET™ Framework technologies

AMULET Cloak™

This application permits the Enmysting™ of a digital asset for full AMULET™ protection independently of any other application or service. The resulting AMULET™-protected digital asset is consistent and compatible with any produced by any other AMULET™-enabled application or service.

AMULET Decloak™

This application permits Unmysting™ of an AMULET™-protected digital asset into persistent storage, when all the criteria of the associated AMULET™(s) are satisfied by the host device's current environment. Note that by prevailing policy, AMULET™-protected digital assets are never permitted to reside unprotected in persistent storage or in memory. Since AMULET Decloak™ specifically enables this capability, all AMULET™s associated with the protection of a digital assets must specifically allow the use of AMULET Decloak™ for Unmysting™ this digital asset if the operation is to be successful.

Hackless Harbor™ isolation environment

This component will be available in application, service, or library form, and can be used by third parties to harness the isolation capabilities of our Code Cocoon™ technologies as an ad hoc callable security feature of their own applications. As a derivative of Code Cocoons™, Hackless Harbor™ can also support operating systems and versions that are different than the host operating system, and among other things can offer the fascinating ability to run snippets of code in Hackless Harbor™'s operating system in real time called from an app in the different runtime operating systems of the device host. Applications could therefore be glued together from a vast variety of apps, scripts, and services from many different operating systems (Hackless Harbor™ will ultimately be made available in several different operating systems that can be run in parallel).

OphGrid™ onboard ecosystem

Think of this component as Hackless Harbor™ on steroids, a computer within a computer - OphGrid provides an entire locked-down ecosystem (sealed operating system within a secure virtual machine) completely detached from any external influence other than gated communications with a specific 'Nomes™-authenticated device and user through AMULET™-protected digital assets. It runs in parallel with your normal operating system, and provides a military-graded safe and secure environment you can switch into and out of at will to perform secure tasks or run discrete background operations. Note that as with Hackless Harbor™, OphGrid™'s operating system can vary from the device host's operating system, and an OphGrid™ instance can support multiple Hackless Harbor™ instances within itself, each potentially running a different operating system or version. This leads to an infinite number of implementation possibilities, especially for testing, experimentation, and comparison purposes.

AMUmail™ - this component will first be made available as a plugin to the Microsoft Outlook™ application (a demo exists now, recorded as a series of videos filmed in Portland, Oregon on the Certitude Digital website), and then will be offered as plug-ins to other popular e-mail clients. There will also be a standalone e-mail client offered. The component offers single-click lock-down AMULET™-enforced security of e-mail components by recipient or recipient groups, easy and automated association of recipient-appropriate AMULET™s for senders, automated (hands-free) Ricochet™ SASE generation of return AMULET™s for the sender of a received e-mail,

and easy access to pre-built community-provided AMULET™s for unknown intended recipients, among other features.

AMUsourcery™

This component (in development now) will initially be offered as plugins to the Visual Studio Integrated Development Environment (IDE) and the Visual Studio Code stand-alone editor. There will also be plugins, add-ons, helpers and scripts for other popular IDEs and editors, as well as a standalone app for directly accessing repositories. These components stop outright the theft of plain-text source code and other resources by Microsoft and others from git and other repositories, notably GitHub, even when Microsoft controls the encryption keys - while of course shutting down any hackers completely, including those who are able to access your local repository, backup, or replication servers.

Parcel Depot™

This is a full-service, full-featured closed-system lockdown-secure digital message and package exchange, drop-off, pickup, publication (both persistent and temporary) and delivery enterprise system, equivalent or superior to the Chinese WeChat application in many ways, with the very important additional feature that each digital item exchanged is fully and independently AMULET™- and 'Nomes™-protected by its originator. The publication of access directories, member information, and published data is likewise under the explicit and exclusive control of the content-providing member. This is the absolutely secure, audit-trailed, members-only replacement for Facebook, Dropbox, Amazon, eBay, GoDaddy, and Ingram, all in one portal, ideal for professionals with fiduciary accountability such as lawyers, doctors, engineers, intellectual property professionals or those invested in any way with I/P, private investigators and law enforcement personnel, among others, who must freely exchange critical information in many forms with their trusted clients and associates. This system can be white-labeled or tailored to individual groups of any kind or size, including social media and special-interest groups, corporations, government entities (including military), non-government organizations (NGOs), and ad hoc collaborations.

AMUbrowser™

This is a browser that, in addition to having all of the features of Google Chrome, is completely secure - individual elements of web pages can be secured as AMULET™-protected digital assets that play or display only if the current user of a devices and its environment pass AMULET™ criteria (all AMULET™-protected digital assets support the option to mount substitute displays or audio the content provider for the digital asset can supply for the unauthorized user as a placeholder).

AMULET Quantum™ multiple-instance user and device representation on remote devices

This is truly revolutionary, all-new, groundbreaking technology that allows projections of your presence on any host device to monitor the usage of your personal or critical data as AMULET™-protected digital assets in individual cells, rows, and columns of foreign, remote databases, or as files or folders in clouds or server farms, without engaging the administrators or owners of those remote services or devices.

This solves in its entirety, with microscopic granularity, the unauthorized use of personal data by entities like Facebook, Google, LinkedIn, Amazon, Microsoft, or IBM, while still allowing all normal behaviors of those systems if (and only if) permitted by the content provider or owner of that data.

This technology generally works as follows (some elements have been left out or described in alternative terms to preserve intellectual property rights in various stages of protection): All data subject to protection is submitted to foreign, remote databases and servers as AMULET™-protected digital assets (MIME64 representations where text-based accessibility is required). The AMULET™(s) protecting those digital assets base their criteria question on the content provider's preferred host device's digital environment. When the database or server encounters AMULET Quantum™-encoded digital assets in a query or read request, the DeviceAgent™ on the database or server host answers the questions posed in the AMULET™ criteria against the context of the digital asset content provider or owner's exported host device environment rather than the database or server host device's digital environment.

Both the database (or server) and the digital access content provider or owner must be logged into authorized accounts on a Certitude Digital environment replication server set up for this purpose. That environment replication server accepts secured copies of the digital asset content provider or owner's current host device's digital environment data as uploaded to it at regular intervals by the DeviceAgent™ on the content provider's device. Authorized applications on other devices having an interest in that environment can download secured copies of it for submission to their DeviceAgent™s, which can then substitute that environment internally for their own when answering an associated AMULET Quantum™ digital asset access request.

The content prover need provide only one regularly uploaded copy of their enciphered digital environment to the environment replication server to support as many AMULET™ Quantum™ digital assets as they happen to have distributed in the wild. Any number of devices wanting to access any one or more of that provider's digital assets can download the environment copy from environment replication server under permission, to the limits of that server's ability to support them.

The content provider can make provisions for the cases where the content provider's device is offline, disabled, or the content provider, which can include seamless transfer between devices, repeating the last known environment with fresh timestamps, or denying digital asset access requests while provider is offline or off the preferred host device.

This mechanism allows the content provider dynamic real-time control of his or her protected digital asset by manipulating their own host device regardless where they reside without having to know or participate in any direct conversation with the remote devices requesting access to a digital asset belonging to the content provider, even when those requests number in the thousands across an equal number of different devices.

A somewhat similar effect can be achieved without AMULET Quantum™ by setting an AMULET™'s criteria to depend upon specific content in a webpage set up for the purpose and accessible by the content provider, but in that case the content provider has to take explicit action to cause changes in the answer received by the AMULET™ criteria. AMULET Quantum™ technologies can trigger off the natural behaviors of the content provider while on his/her device, and do not require any explicit actions from the content provider. Fr example, AMULET Quantum™-friendly AMULET™ criteria could be set to answer "yes" when the content provider's host device GPS location was in New Orleans, and "no" otherwise. A more common scenario would be that the host provider has a list of applications or devices permitted to use a given digital asset as a file in a certain location on his/her host device, and the AMULET Quantum™-friendly AMULET™ criteria would ask "Does my requestor host device and requesting application appear on the replicated environment file's permission list?"

CRD™/DSP™ in-situ realtime copy protection and replication/legacy version discovery

Cellular Replication Discovery (CRD)™ works on the premise that while anyone can easily alter the totality of a file so that it no longer exactly resembles the original, specific subsections of even binary unprotected files remain duplicated in versions of a file that are otherwise vastly different. If enough of these similar sections are present between two candidate versions of a file, the component can safely assume they derived from the same original. The CRD™ tool, then, provides a variety of ways for a user to specify one or more sections of the source file for comparison to sections of other files. It also provides several ways for the comparisons to execute and means for setting tolerances when determining what constitutes a match. CRD™ is described but not detailed in in the "Deaver on Cybersecurity" book (https://www.certitudedigital.com/public_docs/public_doc_book/BookPromoPage.html) in the section "3.1.5.4.2.1 Cellular Replication Discovery (CRD)™ tool" (approximately page 3:207).

Defensive Self-Propagation (DSP)™ allows an AMULET™-protected file to engage the features of Cellular Replication Discovery (CRD)™ as described in the previous paragraph to seek out unprotected digital assets similar to itself in its host environment, report them as desired, and optionally wrap the unprotected digital assets it finds with AMULET™ protection and replace the unprotected file. DSP™ is described but not detailed in in the "Deaver on Cybersecurity" book in the section "3.1.5.4.2.4. Defensive Self-Propagation (DSP)™ design and implementation" (approximately page 3:210).

AMUwallet™

While blockchain ledgers are relatively secure (and can be made more so by the direct use of 'Nomes™ technologies to validate identities of miners, contributors and accessors, along with the use of AMULET™ technologies to secure communications and exchanged digital assets), the interfaces between blockchain ledgers and the analog world, in addition to most of the digital world, are famously not secure (these are the attack points for the most successful hacks against blockchain). AMUwallet™ is the first of several AMULET™-enabled technologies we will be offering to solve these issues, and is specialized to securely store, manage, and exchange Bitcoin and other blockchain currencies.

AMUOfficeLox™

This family of plugins secures the input and output files of all of the components from the various versions of the Microsoft Office™ product suite, automating and enabling full digital asset security via AMULET™-enabled technologies.

... and many more coming!