Limited-Governmental Access To Encrypted Devices V2.0

(proposal)

The following proposal describes, at a high level, and in the broadest of terms, a pragmatic approach to facilitate 'limited-governmental access to encrypted devices'. A key objective of this proposal was to make such access possible but not cheap or easy. This proposal is not an implementation-ready design, and only addresses the extraction of data-at-rest from an encrypted device, and not the extraction of data-in-motion from an encrypted communications channel. It is hoped that this proposal will catalyze global discussions on the subject and eventually lead to a practical solution that is acceptable to all interested parties. This proposal is a wholly original work, and any similarity to other works on this subject is purely coincidental.

V2.0: Content restructured. Proposal simplified and optimized for easier long-term use. Promotional material added.

Introduction

Governments around the world want to be able to easily access data stored on encrypted devices in order to protect their citizens from threats such as terrorism and criminality. However, modern encryption techniques are so secure that it is almost impossible to break through them using a brute-force computational approach, unless unusually small encryption keys have been used. Accordingly, some governments have called for expedited-access mechanisms, commonly known as backdoors, to be added to all encryption algorithms, which would make governmental access to encrypted data relatively easy, perhaps even trivial. The global technology community, along with many other groups that oppose the erosion of civil liberties, has strongly resisted implementing such a solution, as backdoors can be used by both legal and illegal actors, and could ultimately undermine the principle basis of privacy, security and trust in our modern digital world.

In simple terms, nobody wants any government to have free and easy access to their personal data, which is essentially what an encryption backdoor would offer. Nevertheless, in the most exceptional of circumstances, it would seem reasonable that a government's law enforcement or military authorities are able to gain access to data that has been stored on an encrypted device. For example, a terrorist is killed by law enforcement during an act of terror, leaving behind a device that may contain important information about the terrorist's organization and its future plans. Currently, accessing such information on a strongly-encrypted device would be effectively impossible, due the extreme time and cost that would be required to forcibly break through that device's encryption.

Therefore, it is proposed that a different approach be adopted, an expedited one, in which the act of forcibly breaking through a device's encryption is changed from being effectively unaffordable and impossible to merely expensive and hard. The purpose of such an approach is to make the act of brute-force device decryption possible, but not cheap or easy. A non-trivial cost, in both time and money, will be incurred each and every time that it is used, a cost that should be able to restrict its use to only the most exceptional of circumstances.

For example, if it takes 24 hours, using the world's most powerful supercomputer or decryption farm, to forcibly break through a device's encryption then no more than 365 devices could be forcibly decrypted per calendar year (assuming the use of a single decryption resource). Also, at an energy cost of, say, $1 million per decrypted device, most budgets would quickly become exhausted, and when combined with the aforementioned time constraint could cost up to $365 million per year to operate on a continuous basis. Of course, actual times and costs would need to be fine-tuned based on a variety of independently-determined factors. Such times and costs may seem excessively large but when compared to the current situation of not being able to decrypt any strongly-encrypted device within any reasonable timeframe or for any reasonable cost, they would seem to represent a very significant step forward.

Overview

Terminology: Symmetric-key encryption algorithms, such as the Advanced Encryption Standard (AES), use the same key for both encryption and decryption. So, the terms 'encryption key' and 'decryption key' can be used interchangeably.

Brute-force decryption is when encrypted data is decrypted by testing every possible decryption key against that encrypted data until the correct decryption key is found. Such an approach can take a very long time and use a very large amount of energy. If the original encryption key was large enough then brute-force decryption, even using the world's most powerful supercomputers or decryption farms, becomes effectively impossible. However, it is possible to reduce the time and cost of forcibly decrypting encrypted data by using the first part of the encryption key as an advanced starting point.

For example, if data has been strongly-encrypted using a 256-bit encryption key then a standard brute-force decryption would have to test up to 2-to-the-power-of-256 possible decryption keys, which would probably take longer than the current age of the universe and require the use of more energy than that released by a supernova. However, by providing, under very specific, and very controlled, circumstances, a 'partial

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

decryption key', comprised of the first, say, 176 bits of a 256-bit encryption key, only up to 80 bits, or 2-to-the-power-of-80, possible decryption keys will need to be tested, which will reduce the time required to decrypt the strongly-encrypted data to days and the energy required to the output of a typical municipal power plant over the same period.

Exactly just how much a brute-force decryption is 'accelerated' can be controlled by the size of the 'partial decryption key'. The larger the 'partial decryption key' the quicker will be the brute-force decryption, and, conversely, the smaller the 'partial decryption key' the slower will be the brute-force decryption.

Many governments want to be able to forcibly decrypt encrypted data very quickly and easily, which would be equivalent to having a very large-sized 'partial decryption key'. In fact, many governments would very much like to have access to the full decryption key, which would allow encrypted data to be instantly decrypted. On the other hand, a majority of the general public wants it to be very slow and hard for their government to forcibly decrypt encrypted data, which would be equivalent to having a very small-sized 'partial decryption key'. In fact, many members of the general public would not want to give any government, not even their own, any part of any decryption key, which would make brute-force decryption impossible, except for data that had been encrypted using very small-sized encryption keys.

Somewhere in between these two viewpoints lies a realistic compromise, a middle ground, such that, in the most exceptional of circumstances, brute-force decryption of encrypted data will be possible but not so cheap and easy that it can ever become a trivial, everyday, process. The brute-force decryption of encrypted data should always be expensive and hard, and only used after full consideration of the resources that will be consumed in its use.

By using a 'partial decryption key' to accelerate a brute-force decryption it will be possible, by controlling the size of that 'partial decryption key', to ensure that the cost and difficulty of using such a decryption approach will always be sufficiently expensive and sufficiently hard that it can only be used sparingly, in the most exceptional of circumstances, and not as a standard operating procedure for police handling a minor traffic violation or misdemeanor.

This accelerated brute-force decryption approach will, consequently, form the basis of my proposed solution to the 'limited-governmental access to encrypted devices' problem. This solution will be known as Expedited Access to Strongly-Encrypted Devices (EASED).

There are a couple of ways that EASED could be used to solve the 'limited-governmental access to encrypted devices' problem. For example, it could be used in a direct approach to decrypt a device's encrypted data or it could be used in an indirect approach to discover an encryption key-based 'unlock code' that could then be used to initiate a device decryption. Whilst a solution based on a direct approach would be acceptable in many situations, the fact that it allows the encryption key that was used to encrypt a device to become known makes it a less acceptable solution to this particular problem. Therefore, this proposal will use an indirect approach to ensure that no knowledge of the encryption key used to encrypt a device ever leaves that device. However, regardless of how EASED is actually used in practice, it will always make use of a 'partial decryption key' to accelerate a brute-force decryption that will eventually lead to the decryption of an encrypted device.

EASED represents just one possible way that a challenging computation, such as a brute-force decryption, could be used to help solve the 'limited-governmental access to encrypted devices' problem.

EASED is not a backdoor, it does not weaken the encryption algorithms that are used to secure the data stored on our devices, it is simply a method by which a single encryption key-based 'unlock code' for a single encrypted device can be discovered in an accelerated, but non-trivial, manner, and only in very specific, independently validated, circumstances.

EASED's use of an 'unlock code' to initiate a device decryption is very similar to an approach commonly used on many modern devices, which use a user-entered password to initiate a device decryption.

Creating the EASED solution will not require the permission or support of any government. It can be created by any individual, group, or entity, such as the free and open-source software community, or even a leading device manufacturer or global internet company. However, regardless of who eventually develops EASED, they must be fully independent, such that they are free from any governmental influence.

Of course, EASED will first need to be proven to be safe and effective, but once that milestone has been achieved, it can quickly start to be adopted by device manufacturers, and become a viable device decryption option for national governments around the world.

EASED will be offered as a service only to national governments on an as-is, take-it or leave-it basis. EASED may not be the quickest or cheapest solution available but it will be a single generic solution that can reliably work across a wide range of devices. It is, therefore, hoped that EASED will quickly become established as the accepted solution for governmental access to encrypted devices because it will be a ready-to-go solution that represents the path of least resistance for gaining access to such devices. Of course, many other access options will always be open to national governments, but none are expected to offer the relative ease-of-use and consistency-of-operation that EASED will be able to offer.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

Many national governments, perhaps even all national governments, may not like the idea of EASED, as it is described in this proposal, because it has far too many restrictions on how and when it can be used, is not free-of-charge at the point of use, and is not under the direct control of each national government that may wish to use it. However, if EASED was actually made available as a practical decryption option during a time-critical investigation of a crime or terrorist act, and the cost/benefit evaluation was politically favorable, then the use of EASED would be strongly considered, regardless of whether it was liked or disliked by any or all national governments.

EASED is not a perfect solution, it is most definitely a compromise, but it may just be the best compromise currently available.

Challenges (abridged)

The creation and adoption of Expedited Access to Strongly-Encrypted Devices (EASED) will undoubtedly face a number of challenges, such as:

Q1) Can a majority of the general public (device customers) accept that device encryption can be weakened in a safe and controlled manner that cannot be easily abused?

Q2) Can EASED be supported by device manufacturers without negatively impacting their profitability or brand reputation?

Q3) Can partial decryption keys 'related' to encrypted devices, communicated over the internet, be absolutely protected from illegal interception?

Q4) Can partial decryption keys 'related' to encrypted devices be securely stored in an on-line data store such that only the organization responsible for managing that data store can access those keys under any and all circumstances?

Q5) Can the organization charged with managing the global use of EASED operate independently, free from inappropriate third-party influence, particularly from national governments?

Q6) Can government misuse of EASED be avoided?

These challenges are, probably, not insurmountable but neither are they trivial:

A1) Given sufficient time and effort a significant portion of the general public (device customers) can probably be convinced that EASED is a reasonable compromise that will only be used in only the most exceptional of circumstances.

A2) If the answer to question one (Q1) is effectively 'yes' then the negative impact on the brand reputation of device manufacturers that add support for EASED to their devices should be minimal. The cost of adding support for EASED to a device's hardware & software systems, when done at scale, should be relatively small, with the result that the profitability of devices supporting EASED should only be minimally affected.

A3) Techniques and technology for securely communicating cryptographic keys, and a wide range of other data, across the internet are now commonplace and mature, and should, therefore, be reproducible by EASED.

A4) The safe and secure on-line storage and management of cryptographic keys, and a wide range of other data, is now commonplace and mature, and should, therefore, be reproducible by EASED.

A5) Approaches such as virtualization, openness, audit, and the creative use of tools, techniques and technology can all be used to ensure the independence of the organization charged with managing the global use of EASED. For example, virtual-organizations are able to transcend national boundaries and are, consequently, able to operate independently of the national governments of the organization's staff, an approach that should be reproducible by the organization charged with managing the global use of EASED.

A6) By ensuring that the use of EASED is controlled by a fully-independent non-governmental organization the likelihood of governmental misuse of EASED should be greatly minimized.

However, unless all of these challenges can be completely overcome, any attempt to implement EASED will be a dangerous waste of time. EASED can only succeed if it can make a genuinely useful contribution to the fight against crime and terrorism without also broadly degrading civil liberties, which will be a most delicate balance to achieve in practice, but one that must, nevertheless, be achieved if EASED is ever going to become an accepted solution for 'limited-governmental access to encrypted devices'.

Expedited Access to Strongly-Encrypted Devices (simplified)

The way that the Expedited Access to Strongly-Encrypted Devices (EASED) process will work is by providing a national government with a 'partial decryption key' that can then be used to accelerate the brute-force decryption of some encrypted data that is 'related' to a strongly-encrypted device.

The 'partial decryption key' can be used to reduce the computational time and cost of decrypting that data, using a brute-force decryption attack, because a large portion of the computational exploration, the sequential testing of decryption keys, that would normally be required, is avoided.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

Typically, when attempting to forcibly decrypt data that has been encrypted using a modern symmetric-key encryption algorithm, such as the 256-bit version of the Advanced Encryption Standard (AES), speculative 256-bit decryption keys are sequentially created and tested against that encrypted data. If the speculative decryption key is correct then the encrypted data is decrypted. If the speculative decryption key is incorrect then the next speculative decryption key is tried. This process is then repeated until the correct decryption key is found, and the encrypted data has been decrypted.

However, by providing a 'partial decryption key' comprised of the first, say, 176 bits of the original 256-bit encryption key, only the remaining 80 bits of that key will need to be speculatively created and tested, which would significantly reduce the time and cost of forcibly decrypting encrypted data.

The data that EASED will be used to decrypt is of no real importance, other than as the basis of a time-consuming and financially-costly computational challenge that must be solved in order to discover the encryption key that was used to encrypt that data. It is the discovered encryption key that is important, because the sequence of binary digits (bits) that make up that particular encryption key will then be used as an 'unlock code' that will cause a device to decrypt its encrypted data.

The time and cost of solving this computational challenge can be broadly controlled by varying the size of the 'partial decryption key'. The use of a larger-sized 'partial decryption key' makes solving this computational challenge quicker and cheaper. Whilst the use of a smaller-sized 'partial decryption key' makes solving this challenge slower and more expensive. By carefully selecting a suitably-sized 'partial decryption key' it will be possible to make solving this computational challenge sufficiently time-consuming and sufficiently expensive, such that EASED can only be used by a national government in the most exceptional of circumstances.

So, each time a device's data is encrypted using its Device Encryption Key (DEK), a Device Unlock Code (DUC) and some Unencrypted Challenge Data (UCD) will be randomly generated. The DUC, which is also an encryption key, is then used to encrypt the UCD, thereby creating Encrypted Challenge Data (ECD). The DEK, DUC, ECD and UCD will then be securely stored on the device. The DEK and DUC cannot be electronically or physically extracted from the device.

A truncated (tail-shortened) copy of the DUC, known as the Partial Device Unlock Code (PDUC), is then sent, using secure communications, to a secure on-line data storage service, known as the Independent Data Store (IDS). The size (shortness) of the PDUC is defined by the IDS, and must be short enough to incur a minimally-acceptable time and cost in the contemporary use of EASED.

The DEK used to encrypt the device will not be sent to the IDS; it will only ever be securely stored on the device. Only the PDUC will be sent to the IDS.

The IDS will hold the PDUC, in the form of multiple Partial Device Unlock Code Versions (PDUCVs), in escrow until it is requested by a national government. The IDS converts each PDUC into multiple PDUCVs, such that each successive PDUCV will contain one binary digit (bit) less, at the tail-end, of the PDUC than the previous PDUCV. So, if the original PDUC contained 176 bits then the IDS will create 176 PDUCVs that contain truncated (tail-shortened) versions of the PDUC, ranging from the 'first 176 bits of the PDUC' down to just the 'first bit of the PDUC'.

The IDS will only send a PDUCV to a national government when presented with valid legal authorization that was issued by nation-level judicial authorities. The PDUCV will allow a national government to decrypt a device's ECD using EASED, and by so doing discover the DUC that was used to encrypt that data. It is expected that it will take approximately 24 hours and use up to $1 million of energy to discover a DUC using EASED.

Entering the discovered DUC into the encrypted device will then cause that device to decrypt its encrypted data, but only if the discovered DUC exactly matches the DUC previously stored on the device when that device was encrypted. Entry of DUCs will be limited to one per hour.

The PDUCV that the IDS will send to a national government will be one that the IDS has truncated (tail-shortened) such that it will incur a minimally-acceptable time and cost in the contemporary use of EASED.

For clarity, a PDUC is a truncated (tail-shortened) copy of the DUC, which was sent from the device to the IDS, and a PDUCV is a copy of the PDUC that has been further truncated (tail-shortened) by the IDS, which will then be sent to a national government for use with EASED. For example, if a device's DUC was 256 bits long, then the PDUC sent from that device to the IDS might be 176 bits long, and then the IDS might send a PDUCV that is 175 bits long to a national government in order to ensure that the contemporary use of EASED incurs a minimally-acceptable time and cost. The length of the PDUCV sent to a national government is expected to decrease over time.

A minimally-acceptable time and cost is one that is high enough to ensure that EASED will only be used in the most exceptional of circumstances but not so high that its use becomes impractical or so low that its use becomes commonplace.

Determination of the minimally-acceptable time and cost of using EASED will be based on a periodic global-assessment, to be undertaken by the IDS, of the capabilities of the computational resources typically used for EASED (i.e., used for brute-force decryption), such as supercomputers and decryption farms. As such

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

capabilities naturally increase over time the length of the PDUCV made available to national governments will be proportionally decreased, ensuring that a minimally-acceptable time and cost will always be incurred in the contemporary use of EASED.

So, for example, when EASED is first introduced it may use a 176-bit PDUCV and will incur the time and cost associated with speculatively testing the remaining 80 bits of a 256-bit DUC using the computational resources available at that time.

A year later, after the capabilities of the computational resources used for EASED have increased, a 175-bit PDUCV will then need to be used, which will incur the time and cost associated with speculatively testing the remaining 81-bits of a 256-bit DUC, which will probably be very similar to the time and cost that was incurred in speculatively testing 80 bits of a 256-bit DUC using last year's computational resources.

After another year, and a further increase in the capabilities of the computational resources used for EASED, a 174-bit PDUCV will then need to be used, which will incur the time and cost associated with speculatively testing the remaining 82-bits of a 256-bit DUC, and which will probably be very similar to the time and cost that was incurred in speculatively testing 81 bits of a 256-bit DUC using the previous year's computational resources.

So, as the capabilities of the computational resources used for EASED increase over time proportionally-smaller PDUCVs are brought into use by the IDS, ensuring that a minimally-acceptable time and cost will always be incurred in the contemporary use of EASED.

The IDS will permanently remove any PDUCVs held in its data store that are unable to incur a minimally-acceptable time and cost in the contemporary use of EASED.

Current device encryption mechanisms may need to be substantially changed in order to support EASED. Adding specific support for EASED to (personal computing) devices will probably require some hardware changes, and will definitely require some software changes, both of which will require the support of Original Equipment Manufacturers (OEMs) and operating system developers.

Independent Data Store (simplified)

The Independent Data Store (IDS) will be a fully-independent, not-for-profit, non-governmental organization that will be tasked with the secure storage and management of device-related partial decryption keys, known as Partial Device Unlock Code Versions (PDUCVs), which are required to support the use of Expedited Access to Strongly-Encrypted Devices (EASED). The IDS will hold these PDUCVs in escrow until they are requested by a legally-authorized national government.

The IDS will be a hidden TOR (The Onion Router) service that will securely store PDUCVs in a logically-centralized but physically-decentralized manner on multiple globally-distributed computer servers.

The PDUCVs that the IDS will store will be created from the Partial Device Unlock Codes (PDUCs) sent to it from encrypted devices. Each PDUC is converted into multiple PDUCVs, such that each successive PDUCV will contain one binary digit (bit) less, at the tail-end, of the PDUC than the previous PDUCV. So, if the original PDUC contained 176 bits then the IDS will create 176 PDUCVs that contain truncated (tail-shortened) versions of the PDUC, ranging from the 'first 176 bits of the PDUC' down to just the 'first bit of the PDUC'.

PDUCVs will be stored in a segregated manner based on their length. Unacceptably-long PDUCVs stored in the IDS will be securely destroyed, en mass. An unacceptably-long PDUCV is one that is unable to incur a minimally-acceptable time and cost in the contemporary use of EASED.

Each PDUCV will be divided into a number of portions, with each portion being securely stored on a different IDS server. A PDUCV will only be reconstituted when it needs to be sent to a national government. The distributed storage of each PDUCV is intended to add a further layer of protection, above and beyond normal security mechanisms, ensuring that if any one of the IDS servers is successfully compromised then only a small portion of any particular PDUCV can ever be obtained, and which would be insufficient to reconstitute any complete PDUCV. The IDS will keep a detailed audit log of all transactions applied to the PDUCVs within its charge.

The IDS will determine the most appropriate PDUCV to use with EASED based on a periodic assessment of the world's fastest supercomputers and decryption farms, brute-force decryption techniques, and wholesale energy costs, with the objective of ensuring that the contemporary cost of decrypting an encrypted device using EASED will always be highly significant in terms of both time and money, for example, at a minimum of 24 hours and $1 million. Such costs are intended to ensure that EASED will only ever be used in the most exceptional of circumstances.

The software used to implement the IDS will be published under an open-source license so that it can be readily inspected to determine its suitability for use in the protection of potentially hundreds of billions of PDUCVs belonging to billions of encrypted devices. The IDS will utilize existing open-source software wherever possible rather than developing and maintaining its own, although some custom software, particularly for securely storing PDUCVs in a highly obfuscated and decentralized manner, may need to be specially developed.

Only representatives of national governments that have formally registered with the IDS will be able to request

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

PDUCVs from the IDS. The IDS will carefully validate all such registrants. A registration fee may be charged. Registered IDS users will then need to log onto the IDS, via a web portal, in order to submit a legally-valid request for a specific device's PDUCV. The IDS web portal will use multi-factor authentication.

All communications to and from the IDS will use secure communications over obfuscating TOR bridges.

The IDS will only provide a PDUCV to a national government upon receipt of valid legal authorization, issued by nation-level judicial authorities, and communicated over approved communications channels. All PDUCVs so supplied will be short enough to ensure that the contemporary use of EASED will incur a minimally-acceptable time and cost.

Validation of legal authorization will be manual, conducted by legal experts associated with the IDS. The validation process will take at least 24 hours in order to provide the IDS with sufficient time to make its own assessment of the circumstances behind the request, and to ensure that its services are not being misused under legal guise. The time taken to manually validate the legal authorization will also add a tunable delay into the EASED process, which will help to control the rate at which EASED can be used.

The IDS will be wholly independent from any national government and will reserve the right to refuse any request for a PDUCV, at any time, for any reason it deems fit, regardless of whether the request was legally valid. The IDS will have an important and valuable role to play in terms of supporting 'limited-governmental access to encrypted devices' on a global basis, a role that it will professionally undertake at all times, but unless it has the genuine ability to refuse any request for any reason then it will never be truly independent of the national governments that it supports, which is something that it most definitely must be.

Being a not-for-profit organization the IDS will probably need to rely on funding from external sources, such as charitable contributions from the general public, global internet companies or device manufacturers that are happy to have finally been removed from the 'governmental access to encrypted devices' debate. Alternatively, the IDS may need to levy a per-user membership fee or a per-use fee.

Processes

The two principle processes of Expedited Access to Strongly-Encrypted Devices (EASED), device encryption and device decryption, are briefly and simplistically described below. The purpose of these processes is to make governmental access to encrypted devices possible but not cheap or easy. The processes use the following terminology:

- **Device Audit Log (DAL)** contains a permanent record of all device encryption and decryption activity. Displayed on every device start-up or whenever requested by device owner. Used to set DSI. Securely stored on device.

- **Device Encryption Key (DEK)** is the encryption key of the symmetric-key encryption algorithm used to create EDD by encrypting UDD. Randomly generated each time device is encrypted. Securely stored only on device.

- **Device Status Indicator (DSI)** is a colored-padlock graphic that is continuously displayed on a device to visually communicate to a device's owner whether or not a device has been subjected to EASED. A white-colored open-padlock indicates that device data is unencrypted and EASED cannot be applied. A green-colored closed-padlock indicates that device data is encrypted and EASED has not been applied. An orange-colored closed-padlock indicates that device data is encrypted and data required to apply EASED has been extracted from the device. A red-colored open-padlock indicates that device data has been decrypted by EASED. Derived from DAL data.

- **Device Unlock Code (DUC)** is the code that will cause a device to create UDD by decrypting its EDD using its DEK. DUC is an encryption key of the symmetric-key encryption algorithm used to create ECD by encrypting UCD. Can be discovered by applying EASED to ECD using a PDUCV. Randomly generated each time device is encrypted. Securely stored only on device.

- **Encrypted Challenge Data (ECD)** is the encrypted version of UCD. Created by encrypting UCD with the DUC. ECD can be decrypted with DUC. Securely stored only on device.

- **Encrypted Device Data (EDD)** is the encrypted version of UDD. Created by encrypting UDD with DEK. EDD can be decrypted with DEK. Stored on device.

- **Expedited Access to Strongly-Encrypted Devices (EASED)** is a brute-force decryption technique that uses a 'partial decryption key' to accelerate its operation. Designed to always incur a minimally-acceptable time and cost in its contemporary use. A 'limited-governmental access to encrypted devices' solution. Includes the operation of the IDS.

- **Independent Data Store (IDS)** is a fully-independent non-governmental organization and secure data storage service. Converts PDUCs into multiple PDUCVs. Manages storage of PDUCVs. Controls access to PDUCVs. Sends a PDUCV to a

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

national government when legally authorized. Defines the PDUCMS.

- **Legal authorization** is a permission that was lawfully issued by a nation-level judicial authority to a national government allowing that government to apply EASED to an encrypted device that is in the legal physical-possession of that government.

- **Partial Device Unlock Code (PDUC)** is a truncated (tail-shortened) copy of the DUC. Content of PDUC is controlled by PDUCMS. Sent to the IDS for processing. Converted into multiple PDUCVs by the IDS. PDUC exists only temporarily and is not permanently stored anywhere.

- **Partial Device Unlock Code Max Size (PDUCMS)** is the maximum number of binary digits (bits) of the head-end of the DUC that should be stored in the PDUC. Defined by the IDS. Sent to device by the IDS when requested by device encryption process. Securely stored on the IDS.

- **Partial Device Unlock Code Version (PDUCV)** is a truncated (tail-shortened) copy of the PDUC. Sent to a national government by the IDS. Used to discover DUC by applying EASED to ECD. Multiple PDUCVs created from a single PDUC by the IDS such that each successively created PDUCV is one binary digit (bit) smaller, at the tail-end, than the previously created PDUCV. Securely stored only on the IDS.

- **Secure Non-Volatile Memory (SNVM)** is a device's tamperproof random access memory-based data store. Data stored within SNVM is retained even when a device is powered off. Electronic access to data stored within SNVM is restricted, by device hardware, to approved processes only. Physical access to data stored within SNVM is impractical due to its construction. Used to securely store DAL, DEK, DUC, ECD and UCD. Also used to securely store temporary data created during device encryption and decryption.

- **Securely communicated** is used to describe data-in-motion, between a source and a destination, carried over a continuously-encrypted communications channel. Access to securely-communicated data is restricted to authorized processes and entities only.

- **Securely stored** is used to describe data-at-rest in a continuously-encrypted data store. Such data may also be electronically and physically protected. Access to securely-stored data is restricted to authorized processes and entities only.

- **Unencrypted Challenge Data (UCD)** is the unencrypted version of challenge data. Randomly generated each time device is encrypted. Can be recreated by decrypting ECD using DUC. Securely stored only on device.

- **Unencrypted Device Data (UDD)** is the unencrypted version of a device's data. Can be recreated by decrypting EDD using DEK. Stored on device.

- **Unique Device Identifier (UDI)** is a code that uniquely identifies a device. Randomly generated each time device is encrypted. Securely stored on the device.

The following processes assume that the DEK and the DUC are securely protected by hardware-based security at all times, and cannot be physically or electronically extracted from a device; they are only accessible by the device's cryptographic systems. Also, the only EASED-related data that can be manually extracted from a device are the ECD, UCD and UDI. An encrypted device will only create UDD by decrypting its EDD using its DEK when a valid DUC has been input into that device. A symmetric-key encryption algorithm, such as the 256-bit version of the Advanced Encryption Standard (AES), will be used to secure all critically-important data elements. All device encryption and/or decryption activity will be recorded in the DAL. Whether or not EASED has been applied to a device will be indicated by the permanently displayed DSI, and also by the display of the DAL on every device start-up.

The following process descriptions are highly simplistic, and lack, amongst other things, any error handling. If a process should fail then it should be assumed that it will always fail safely, ensuring that encrypted data always remains encrypted. The use of encryption initialization vectors (IVs) is assumed but not described. An actual implementation of these processes is expected to be far more complicated than what has been described below, particularly given the need to adequately secure all critically-important data elements at all times (i.e., at-rest, in-motion and in-use).

Device encryption (simplified):

This process is used when a device is to be encrypted or re-encrypted.

1) If current Device Encryption Key (c-DEK) exists in device's Secure Non-Volatile Memory (SNVM) then create Unencrypted Device Data (UDD) by decrypting Encrypted Device Data (EDD) using c-DEK, and then securely destroy c-DEK.

2) Randomly generate a new Device Encryption Key (n-DEK) and store it in SNVM.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

3) Create EDD by encrypting UDD using n-DEK.

4) Randomly generate new Device Unlock Code (n-DUC).

5) Randomly generate new Unencrypted Challenge Data (n-UCD) and store it in SNVM.

6) Create new Encrypted Challenge Data (n-ECD) by encrypting a copy of n-UCD using n-DUC and store it in SNVM.

7) Obtain the latest Partial Device Unlock Code Max Size (PDUCMS) value from the Independent Data Store (IDS) using secure communications.

8) Let *x* equal the value of PDUCMS. Create new Partial Device Unlock Code (n-PDUC) containing the first *x* binary digits (bits) of n-DUC.

9) Randomly generate a new Unique Device Identifier (n-UDI) and store in SNVM.

10) If current Unique Device Identifier (c-UDI) exists in SNVM then obtain a copy of c-UDI, otherwise set c-UDI to NULL.

11) Send a copy of the c-UDI, n-UDI, and n-PDUC by secure communications to the IDS for processing. IDS converts n-PDUC into multiple Partial Device Unlock Code Versions (PDUCVs). IDS securely stores the PDUCVs based on n-UDI, segregated by PDUCV size. IDS securely destroys n-PDUC. If c-UDI is not NULL then the IDS will securely destroy any PDUCVs associated with c-UDI that are currently stored in the IDS.

12) If c-UDI is not NULL then securely destroy c-UDI.

13) If current Device Unlock Code (c-DUC) exists in SNVM then securely destroy c-DUC.

14) If current Encrypted Challenge Data (c-ECD) exists in SNVM then securely destroy c-ECD.

15) If current Unencrypted Challenge Data (c-UCD) exists in SNVM then securely destroy c-UCD.

16) Securely destroy n-PDUC. Rename n-DEK as c-DEK. Rename n-DUC as c-DUC. Rename n-ECD as c-ECD. Rename n-UCD as c-UCD. Rename n-UDI as c-UDI.

17) Record details of device encryption activity in Device Audit Log (DAL). Device Status Indicator (DSI) set to a green-colored closed-padlock.

18) End.

Device decryption (simplified):

This process is used when an encrypted device, which is in the legal physical-possession of a national government, is required to be decrypted using Expedited Access to Strongly-Encrypted Devices (EASED).

1) National government has legal physical-possession of the encrypted device to be decrypted by Expedited Access to Strongly-Encrypted Devices (EASED). Device Status Indicator (DSI) is a green-colored closed-padlock graphic.

2) National government physically disassembles device in order to gain access to the device's EASED interface.

3) National government extracts Unique Device Identifier (UDI) from device via EASED interface. Device automatically logs time and date of UDI extraction in Device Audit Log (DAL). DSI is set to an orange-colored closed-padlock graphic.

4) National government obtains legal authorization from nation-level judicial authorities to apply EASED against encrypted device identified by UDI.

5) National government logs onto the Independent Data Store (IDS) web portal, submits legal authorization and UDI to the IDS.

6) IDS validates legal authorization and determines whether this specific use of EASED is reasonable. Minimum of 24 hours elapses.

7) If legal authorization is valid and this specific use of EASED is reasonable then a Partial Device Unlock Code Version (PDUCV) for the device identified by the supplied UDI will be sent by secure communications from the IDS to the national government, otherwise go to step 11. *Note: The PDUCV that will be sent will be one that is short-enough to incur a minimally-acceptable time and cost in the contemporary use of EASED.*

8) National government extracts Unencrypted Challenge Data (UCD) and Encrypted Challenge Data (ECD) from device via EASED interface. Device automatically logs time and date of UCD and ECD extraction in DAL. DSI is set to an orange-colored closed-padlock graphic.

9) National government uses the PDUCV to apply EASED to the ECD in order to decrypt it. When decrypted ECD exactly matches UCD then decryption is complete, and Device Unlock Code (DUC) is discovered. It is expected that it will take the national government approximately 24 hours to discover the DUC using a highly-capable computational resource.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

10) National government enters discovered DUC into device via EASED interface. If discovered-DUC is exactly the same as DUC-stored-on-device then device uses its Device Encryption Key (DEK) to decrypt its Encrypted Device Data (EDD), thereby creating Unencrypted Device Data (UDD), device automatically logs time and date of DUC entry and EDD decryption in DAL, and DSI is set to a red-colored open-padlock graphic. It is expected that it will take a few hours for the device to decrypt its EDD.

11) End.

Advantages and disadvantages (abridged)

In terms of advantages and disadvantages, the proposed Expedited Access to Strongly-Encrypted Devices (EASED) approach, described above, has a number of both, some of which are now listed below.

Advantages:

- The Independent Data Store (IDS) will not be run by any government; it will be run by a fully-independent, not-for-profit, non-governmental organization.

- EASED represents the middle ground in the current 'governmental access to encrypted devices' debate, which has become increasingly polarized into 'all or nothing' viewpoints, by offering a viable alternative to either placing backdoors into all current and future encryption algorithms or completely blocking governmental access to encrypted devices.

- EASED will not weaken any encryption algorithm; it is simply a method to accelerate the discovery of an encryption key-based 'unlock code', on one device at a time, in a very controlled manner.

- EASED will be compatible with most, if not all, modern symmetric-key encryption algorithms.

- No part of the encryption key used to encrypt a device ever leaves that device.

- EASED will only support full-device decryption and not partial-device decryption (i.e., individual data files cannot be selectively decrypted).

- EASED can be selectively applied to one class of devices, such as those used by non-governmental users and excluded from another class of devices, such as those used by governmental users.

- EASED has limited scope in that it is only applicable to data-at-rest on an encrypted device and is not applicable to data-in-motion over an encrypted communications channel.

- EASED is not intended to be a solution to the 'limited-governmental access to encrypted devices' problem that can work remotely, over a communications channel such as the internet, and it will be specifically engineered to enforce such limitations wherever possible.

- The contemporary use of EASED always incurs a minimally-acceptable (non-trivial) time and cost.

- EASED will not support mass surveillance because it will require the legal physical-possession of each device, unique legal authorization for each device, use of a powerful decryption resource, per device cooperation of a fully-independent third-party, and will operate in a time consuming and expensive manner; none of which are practical at anything other than the smallest of scales.

- Using EASED to decrypt any one encrypted device will have no impact on any other encrypted device; each device is separate and unique as far as EASED is concerned.

- EASED requires that each and every device to be decrypted using EASED must be in the legal physical-possession of the national government that needs to decrypt it.

- The data required to apply EASED against an encrypted device can only be obtained from that device via a dedicated interface, which can only be accessed by physically disassembling that device.

- The use of EASED must be legally authorized by nation-level judicial authorities on a per device basis.

- Use of EASED will be restricted to approved users that are only able to communicate with the IDS over approved channels. Only the official representatives of national governments can become approved users.

- EASED will be adaptive; proportionally reducing the acceleration of its brute-force decryption mechanism as global computing power grows.

- The IDS will never have physical or remote access to any device that is subject to the legally-authorized use of EASED, or to the encrypted or decrypted data of such a device.

- IDS systems will be based on open-source software, which will allow the design of those systems to be inspected to determine suitability for purpose.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

- EASED will be designed to fail safely, ensuring that encrypted data will never become decrypted unless all required operating procedures have been followed correctly.

- All transactions, such the storage, reconstitution, and deletion of partial decryption keys 'related' to encrypted devices, undertaken by the IDS, will be recorded into a secure audit log.

- Any and all EASED-related activity that occurs on an encrypted device will be automatically logged in a Device Audit Log (DAL), which will then be permanently and securely stored on that device. The contents of the DAL will be displayed on each device start up, or whenever required, thereby ensuring that EASED cannot be applied secretly.

- A permanently-displayed graphical indicator will be used to visually communicate to a device's owner whether or not that device has been decrypted using EASED, thereby ensuring that EASED cannot be applied secretly.

- The IDS will be a one-stop-shop for national governments that effectively removes all other parties, such as device manufacturers, operating system developers, and telecommunications companies, from the process of gaining access to encrypted devices that support EASED. When a particular encrypted device that supports EASED needs to be accessed a national government will only need to liaise with the IDS and no one else.

Disadvantages:

- The IDS will be a fully-independent, not-for-profit, non-governmental organization that will probably need external funding in order to operate, funding that could lead to undue influence over its operations by its funders.

- Partial decryption keys 'related' to encrypted devices will be communicated across the internet, to and from the IDS, and could be illegally intercepted by bad actors.

- Partial decryption keys 'related' to encrypted devices will be stored on-line, in the IDS, and could be vulnerable to electronic attack by bad actors.

- IDS systems will use open-source software, which bad actors could use to gain a detailed understanding of its operation, by studying its publically available design documents, with the aim of disrupting its operation or stealing partial decryption keys.

- EASED will essentially be a single solution with global applicability that effectively puts all our eggs (partial decryption keys) into a single basket. When highly valuable data is concentrated into a single place it can become very tempting to bad actors.

- EASED is, as a whole, a relatively complex solution, and complex solutions are often significantly more risky than simple solutions.

By seeking to fully understand all of the advantages and disadvantages of EASED, it should be possible to maximize the advantages and mitigate the disadvantages. With the result that the final EASED solution will be far better suited to its intended purpose, in terms of fit, form and function.

Fictional promotional material

Some fictional promotional material has been included below to illustrate how the proposed 'limited-governmental access to encrypted devices' solution could potentially be promoted to national governments. This material uses the following user-friendly terminology:

- **EASED™ Device Solution** is the hardware and software that must be installed inside a device in order to be able to use EASED on that device. Only discussed indirectly within this proposal.

- **EASED™ Accelerator** was previously described within this proposal as the Partial Device Unlock Code Version (PDUCV).

- **EASED™ Unlock Code** was previously described within this proposal as the Device Unlock Code (DUC).

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

EXPEDITED ACCESS to STRONGLY-ENCRYPTED DEVICES™

(EASED™)

WHAT

An expedited solution for limited-governmental access to encrypted devices.

WHY

In the most exceptional of circumstances, such as when investigating a serious crime or terrorist act, it may be necessary to gain access to data stored on a strongly-encrypted device. Without EASED™ such access would be impossible.

WHO

EASED™ has been specifically designed for use by national governments.

HOW

1. Gain legal physical-possession of the encrypted device *(which must contain the EASED™ Device Solution)*.
2. Obtain legal authorization to use EASED™ against the encrypted device.
3. Submit legal authorization to Independent Data Store (IDS) Web Portal *(registration required)*.
4. Wait while legal authorization is validated by IDS *(approx. duration: 24 hours)*.
5. Receive EASED™ Accelerator from IDS.
6. Generate EASED™ Unlock Code by using EASED™ Accelerator with EASED™ *(approx. duration 24 hours)*.
7. Activate device decryption by entering EASED™ Unlock Code into device *(approx. duration: 3 hours)*.
8. Access decrypted device data.

PERFORMANCE

If you started using EASED™ on Monday morning the whole process, from step 1 to step 8, should be finished by no later than Friday evening.

NOTES

Total elapsed time per decrypted device: 120 hours (estimated), 5 full days (estimated), midnight on Sunday night to midnight on Friday night (estimated). Cost per decrypted device: $1 million (estimated), mainly due to the cost of operating the computational resource used for EASED™. Computational Resource for EASED™: Supercomputer - world's top 10 fastest (minimum) or dedicated decryption farm (recommended). Multiple simultaneous uses of EASED™ will require the simultaneous use of multiple computational resources suitable for EASED™. User of EASED™ is responsible for providing all computational resources required for EASED™. Encrypted Device: Must contain the EASED™ Device Solution hardware and software. About IDS: Independent Data Store (IDS) is a fully-independent not-for-profit non-governmental organization responsible for the secure storage of EASED™ Accelerators and for globally overseeing the appropriate use of Expedited Access to Strongly-Encrypted Devices™ (EASED™). IDS Web Portal Registration: All registrants must meet all membership criteria specified by IDS. Access to IDS Web Portal requires multi-factor authentication. IDS Web Portal Registration fee of $1 million payable in advance. IDS Web Portal membership fee of $1 million per registrant payable annually, waived in first year. Payments: All fees paid to IDS are non-refundable. Limitations: EASED™ is an expedited solution for limited-governmental access to encrypted devices that typically takes the greater part of a week to gain access to an encrypted device; it is not a real-time solution. Although EASED™ is a mature and field-proven solution for limited-governmental access to encrypted devices absolutely no guarantees are offered or implied relating to outcomes from using EASED™. IDS reserves the right to not cooperate with any national government's use of EASED™ for any reason. Reasons for such non-cooperation will be shared at the sole discretion of IDS. The EASED™ service may be withdrawn at any time without warning or explanation. Disclaimer: IDS accepts no liability whatsoever relating to any loss real or imagined relating to the use of EASED™ and IDS systems. The 'Expedited Access to Strongly-Encrypted Devices' name and the 'EASED' acronym are trademarks of Independent Data Store. © Copyright Independent Data Store. All rights reserved.

FICTIONAL PROMOTIONAL MATERIAL

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=