INTRODUCTION

This document contains a list of terms pertaining to the use of 1-Wire® SHA-1 devices such as the DS1963S, DS1961S, and DS2432. Every effort is being made to make the terms in the various application notes and data sheets consistent. When that is not possible, alternate terms are provided in the definitions. *(Special terms, commands, or codes are shown in italics for clarity)*.

Authenticate	A process to verify whether something is genuine. (see *Challenge and Response*)
Authentication InputSecret	The input data that is used to compute the *Master Authentication Secret* using the *Compute First Secret* command of the DS1963S. The input data should be 47 bytes in length (or multiples of 47 bytes, where each 47-byte block after the first is processed with the *Compute Next Secret* command). The first 32 bytes are written to a memory page and the last 15 bytes are written to the scratchpad. For the resulting secret to be compatible with the secret generated by the DS1961S, it is essential that first 4 bytes and the last 3 bytes of the 15-byte block written to the scratchpad be FF (hex). Also known as: Input Authentication Secret
Authentication Page	Memory page in the DS1963S when used as a coprocessor that is associated with the secret containing the *Master Authentication Secret*. It can be any arbitrary page except 0 or 8. This page is used in the construction of the *Unique Authentication Secret* of a token. This reconstructed UAS is saved in the *Workspace Secret* of the coprocessor.
Authentication Secret	The secret data that is used as input to the generation of the authentication MAC by a token. This secret data could be unique as in the *Unique Authentication Secret* or it may be the same for each token. Note that this is different than the *Authentication InputSecret*. Also known as: Device Authentication Secret, Device Secret
Authentication Target	The object that is to be authenticated. This could be a person, message, or a token.
Binding Data	The 32-byte data block that is loaded into the token when binding the *Master Authentication Secret* to the token to create the *Unique Authentication Secret*.

1-Wire is a registered trademark of Dallas Semiconductor.

Binding Page Number	The token page number that is used when binding the *Master Authentication Secret* in the token to create the *Unique Authentication Secret*. This page number is one byte in the *Partial Binding Code*.
Challenge and Response	Authentication scheme where a host presents a challenge and the Authentication Target provides a response. If the correct response is given then the target is judged authentic. (see A*uthenticate*)
Class Break	Event that occurs when information has been obtained that compromises the security of an entire system or service. This could happen if the *Authentication Secret* in a system is not made unique to each token and was revealed. (see *Unique Authentication Secret*)
Coprocessor	Extra processor that does a special task. In the context of *SHA-1* operations, a coprocessor must keep secrets secure and perform SHA-1 calculations to compute MACs for authentication of devices and validation of data. (see *Master Authentication Secret, Master Signing Secret*)
Debit/Credit	Process of reducing or increasing the monetary value of an *eCertificate*. (see *eCertificicate*)
eCash	A service that allows the transfer of monetary value using electronic tokens.
eCertificate	*Service Record* data structure for electronic representation of money in an electronic token. Refer to Application Note 151. Also known as: Digital Monetary Certificate
Emulate	To imitate the operation of a device to equal the original's operation. This is only useful in the context of 1-Wire *SHA-1* devices if the Authentication Secret is known. (see *Authentication Secret*)
Entropy	Measure of disorder and randomness. When creating random challenges for doing Authentication, they should be selected with high entropy.
Hash	A constant length distillation of a message. (see *SHA-1*)

Initial Signature	The 20-byte padding data that is used in lieu of a real *Service Data Signature* when computing the signature to be embedded in a service record. This data is often constant for a given system.
InputSecret	Data input that is used in secret generation. For the 1-Wire *SHA-1* devices, the generation of a secret involves running the *SHA-1* engine on this input data. (see *Authentication InputSecret*, *Signing InputSecret*)
MAC	Message Authentication Code. A *Hash* where some of the input data is secret.
Master Authentication Secret	Secret used in the building of a *Unique Authentication Secret* for authentication of a token. This can be stored in any secret location except *Secret 0* of a DS1963S when used as a coprocessor. Also known as: System Authentication Secret, MAS
Master Signing Secret	Secret used in the generation of a *Service Data Signature* MAC for verification of *Service Data*. This is stored in *Secret 0* of a DS1963S when used as a coprocessor. This secret is never stored in a *User Token*. Also known as: Monetary Secret, MSS
Monetary Units Code	Field in an *eCertificate* that specifies the type of money being represented. Follows ISO standard 4217. Using in conjunction with multiplier for scaling. (see *eCertificate*)
Page Number	The 1-Wire devices with memory are divided into pages by convention. Page number counting starts at zero. On the *SHA-1* devices, some memory pages are associated with a write-cycle counter and/or secret.
Partial Binding Code	The 7-byte data block which is loaded into the scratchpad of the token before computing the *Unique Authentication Secret*. The other eight bytes of the scratchpad are the *ROM ID* of the device and the *Authentication Page* number. This, along with *Binding Data*, is used with *Master Authentication Secret* to create the *Unique Authentication Secret*. (see *Binding Data, Unique Authentication Secret*)

Partial InputSecret	Same as *InputSecret* except the *SHA-1* calculation is performed multiple times with different input data. Security is improved if the InputSecret data is split between several people. The secret can then only be created when all pieces are brought together. Not to be confused with the two different pieces that make up each *InputSecret* in the DS1963S, 32 bytes in the memory page, and 15 bytes in the scratchpad. Also known as: Partial Secret
Password/PIN/Passphrase	Data supplied by a user for authentication. Can be used as a *Partial InputSecret*. *Passphrase* usually refers to a very long password.
Pseudorandom	A value that appears random but is actually deterministic from previous values. A good Pseudorandom generator has a very large period before repeating.
ROM ID/ 1-Wire Network Address	Unique number lasered into all 1-Wire devices. Contains an 1-byte family code to identify the type, 6-byte serialization number, and 1-byte CRC verification. Also known as: iButton Address®, Serial Number, Address Number, Registration Number, ID, Unique ID
Salt	Random value added to a data block before a MAC signature for validation is created. This makes the signature different even when the data block remains the same. The *Transaction ID* field in the *Service Data* serves this purpose. (see *Transaction ID*)
Secret Write-Cycle Counter	A counter associated with an individual secret that increments whenever the secret is written on the DS1963S. It does not roll over or reset. Can be used to verify that a secret has not been tampered with.
Secret	Portion of the input block to the *SHA-1* calculation that is known only to participants in a *Service*. The participants include the *User Tokens* and the *Service Control Unit*. (see *Unique Authentication Secret, Master Signing Secret*)
Secret 0	Secret associated with memory page eight on the DS1963S. This secret has a special feature, which allows the SHA-1 calculation result to be read out. For this reason, this secret is used in coprocessor operations to generate *Service Data Signatures*. For security reasons this secret should not be used for doing device authentication.

Secret Rotation	A methodology to change the secrets in a system to increase security periodically or in response to a breach. Must be carefully designed into a system before implementation.
Service	Providing for some need or function (e.g., vending).
Service Control Unit	Microprocessor or computing device that handles that authentication of a token and validation of its data. It also performs the service (e.g., dispensing candy, opening a door).
	Also known as: Transactor, Host, Authentication Host, Local Host, SCU Transaction Control Unit (TCU).
Service Data	Data that resides on the token that makes it part of a service. It will include a *Transaction ID* and optionally a *Service Data Signature*. An eCertificate is an example.
	Also known as: User Data, Application Data, Account Data, Transaction Data
	(see *eCertificate, Transaction ID, Service Record*)
Service Data Signature	MAC that is included in the *Service Data* and validates the *Service Record*. The *Service Control Unit* creates the signature with the *Master Signing Secret*.
	Also known as: Data Signature, Message MAC, Signature MAC, Embedded Service Data Signature
Service Provider	Entity that provides a service.
	(see *Service*)
Service Record	The file that contains the *Service Data* on a token.
	Also known as: Account File, Purse File
SHA-1	Secure Hash Algorithm specified in the Federal Information Publication 180-1 (FIPS 180-1).
	(see *Hash*)
Signing Challenge	The 3-byte data block, which is loaded in lieu of a real challenge into the scratchpad locations 20 to 22 of a DS1963S coprocessor before computing the *Service Data Signature* to be embedded in a *Service Record*. This data is often constant for a given system.

Signing InputSecret	The input data that is used to compute the *Master Signing Secret* using the *Compute First Secret* command of the DS1963S. The input data should be 47 bytes in length (or multiples of 47 bytes, where each 47-byte block after the first is processed with *the Compute Next Secret* command). The first 32 bytes are written to a memory page and the last 15 bytes are written to the scratchpad. Also known as: Input Signing Secret
Signing Page	Page 8 of a DS1963S when used as a coprocessor. It has the special feature of allowing the SHA-1 signature to be read out. This page along with its associated secret (*Secret 0=Master Signing Secret*) is used to create *Service Data Signatures.* This page and its associated secret (*Secret 0*) is never used for *Service Data* in *User Tokens*.
Token	Portable representation of value. Also known as: Roving iButton, Dallas Electronic Token, user device, portable token, and SHA iButton
Transaction ID	*Salt* field in the *Service Data* to make each instance of a *Service Record* unique. (see *Salt, Service Data*)
Unique Authentication Secret	Authentication secret that is made unique for each device by including the unique *ROM ID* as part of the data used to calculate the secret (*Partial Binding Code*) from the *Master Authentication Secret*. Also known as: Unique Token Secret (UTS), UAS (see *Partial Binding Code, Master Authentication Secret*)
User Token	Token issued to an end user in a *Service*. When the token is an iButton it can be referred to as a *User iButton*.
Workspace Page	Arbitrary page in a DS1963S coprocessor (1 to 7 and 9 to 15) that is associated with the generated *Unique Authentication Secret*. This page is only used temporarily while authenticating a token.
Workspace Secret	Temporary secret that contains the generated *Unique Authentication Secret* in a DS1963S coprocessor.
Write-Cycle Counter	A counter that increments whenever data is written to the associated page. It does not roll over or reset. Used in verification of *Service Data* to prevent data replay.