

# Ensuring Token Reliability Across the Enterprise

Token reliability is a critical foundation for enterprise security. Organizations that deploy hardware-based authentication tokens want to ensure that users are indeed who they claim to be, and they want the users to experience the best possible quality from the product. But these tokens over the course of their useful life are often subject to abuse and neglect.

RSA Security continues to invest in delivering the most reliable hardware tokens in the industry, and this white paper provides an overview of the rigorous reliability testing RSA Security conducts to ensure that our tokens stand up to some of the most demanding conditions imposed on them by users throughout the enterprise.

TABLE OF CONTENTS

I. TOKEN RELIABILITY IS KEY TO SUCCESSFUL SECURITY IMPLEMENTATIONS	PAGE 1
II. HIGHLY RELIABLE AUTHENTICATION TOKENS	PAGE 1
III. CHALLENGING CONDITIONS ARE INEVITABLE	PAGE 2
RSA SecurID 700	PAGE 2
The RSA SecurID 800 Connected Authenticator	PAGE 2
IV. INVESTING IN TOKEN RELIABILITY	PAGE 2
V. TEMPERATURE, HUMIDITY AND ALTITUDE TESTING	PAGE 3
VI. VIBRATION, SHOCK, DROP AND TUMBLE TESTING	PAGE 3
VII. ELECTROSTATIC DISCHARGE TESTING	PAGE 4
VIII. RUGGEDNESS CHECKS	PAGE 4
IX. CONCLUSIONS	PAGE 5
About RSA Security	PAGE 6

## I. TOKEN RELIABILITY IS KEY TO SUCCESSFUL SECURITY IMPLEMENTATIONS

Organizations that deploy two-factor authentication are able to secure access to enterprise information and applications while providing users with convenient and easy-to-use tokens that allow them to authenticate to enterprise resources. Hardware tokens have been designed to be small enough to easily attach to a key chain. Most of these tokens will likely have a useful life from three-to-five years, so they should be designed to ensure maximum reliability even under the most challenging conditions.

A failed token not only results in loss productivity by the user; it also increases help desk costs and burdens the enterprise to stock and distribute excessive numbers of spare tokens. Token reliability is a key to providing the user with a positive and productive security experience; it is also essential for driving down the total cost of ownership (TCO) of enterprise security.

Over the life cycle of a token, it is likely to be exposed to extreme conditions—any one of which can potentially damage the token, leaving the user without access to enterprise information and resources. Many of these extreme conditions can be predicted, and tokens can be routinely tested to ensure industry-leading levels of reliability.

For example, tokens could be exposed to extreme temperature and humidity conditions or to the altitude pressures of being in a cargo bay of an airplane. They could also be subject to extreme vibration or shock conditions, or could just be dropped out a window or off a desk. Electrostatic Discharge (ESD) is another common threat to token reliability, and ruggedness is critical so that tokens

can withstand the inevitable bangs, bruises and scrapes that they will experience as a result of potentially being carried by users seven-days-a-week throughout their busy lives.

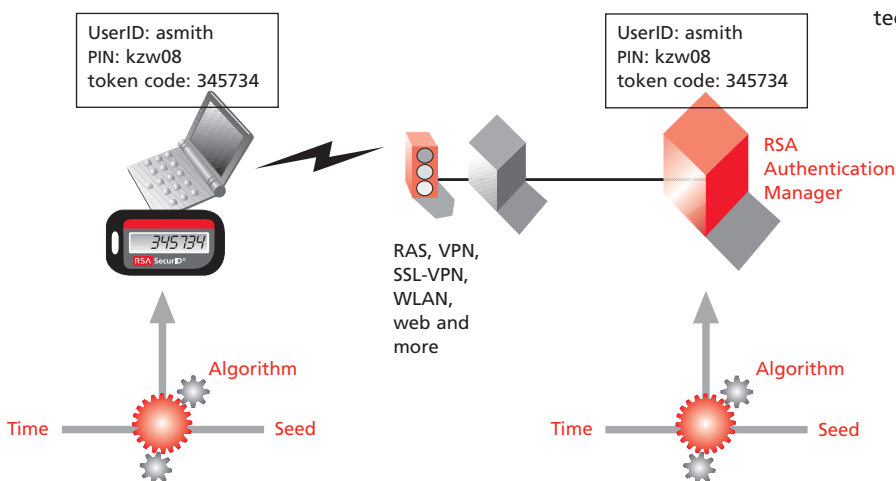
Certain “unpredictable” abuse conditions can also be predicted. Some tokens will be left in clothes and run through washing machines—and clothes dryers. They will be run over by cars, dropped into sinks and left on top of hard drives. Not all tokens are created equal. Reliability is not a by-product of design, but rather a goal of design.

RSA Security invests heavily in token reliability so that organizations can simplify the management of security infrastructure and resources. We offer industry-leading levels of reliability, and our tokens are designed to withstand the worst imaginable conditions. By selecting SecurID® authentication tokens from RSA Security, organizations can increase workforce productivity by distributing the most reliable tokens in the industry. They can reduce the overhead costs of distributing replacement tokens, and they can drive down the overall cost of security while providing a consistent and easy-to-use authentication experience for end-users.

## II. HIGHLY RELIABLE AUTHENTICATION TOKENS

RSA SecurID® two-factor authentication solutions are based on something you know—a password or Personal Identification Number (PIN)—and something you have—an authentication token that generates a constantly changing code. To access resources protected by RSA SecurID technology, a user simply combines his or her secret PIN with the token code generated by their RSA SecurID authenticator.

Based on RSA Security’s patented time-synchronous technology, RSA SecurID authenticators generate a simple one-time authentication code that changes every 60 seconds. This unique one-time use passcode is used to positively identify—or authenticate—the user. The token code on the authentication device is synchronized with a centralized RSA® Authentication Manager, and if the passcode created by a combination of the PIN and token code are validated by the RSA Authentication Manager, the user is granted access to the protected resource.



RSA SecurID TIME-SYNCHRONOUS  
TWO-FACTOR AUTHENTICATION

If the passcode is not recognized, access is denied. This is a simple-to-use security solution based on extremely sophisticated authentication technology and it has to work right the first time, and every time. Users rely on their authentication tokens to access everything from their Windows computers to web servers. The tokens can enable secure remote access to the enterprise, and secure wireless connections to enterprise applications and information. RSA Security offers a range of authentication options, including both software-based and hardware-based authenticators.

### III. CHALLENGING CONDITIONS ARE INEVITABLE

Despite the best efforts of security personnel and IT staff, end-users will inevitably impose challenging conditions on their authentication devices. Whether that means the devices will go through laundry cycles, get run over by a car, get exposed to X-rays at the airport, get swung from a key chain for hours a day, or left in a car in the freezing cold or the sweltering heat, the tokens must withstand these conditions if the enterprise is going to truly reap the rewards of investments in enterprise security infrastructure. The white paper focuses on the reliability testing for two leading hardware tokens from RSA Security.

#### RSA SecurID 700

The RSA SecurID 700 device is a small key fob model that connects easily to any key ring and is very convenient for the end-user. It displays a unique code generated by the RSA SecurID algorithm every 60 seconds for the programmed life of the fob.

#### The RSA SecurID 800 Connected Authenticator

The RSA SecurID 800 connected authenticator is a multi-function device that combines the industry proven features of the RSA SecurID Hardware Authenticator with a smart chip based on SUN® Java® technology, packaged together in a very convenient USB form factor that includes a display. This authenticator plugs into any USB device to support anytime, anywhere access, and it also supports digital signatures and file encryption certificates. It securely stores password information, making it an ideal choice for a wide range of environments where diverse system, application and customer needs exist. It can either be used as a standalone token or it can be used as a connected token by plugging it into a USB port.



RSA SecurID 700



RSA SecurID 800

### IV. INVESTING IN TOKEN RELIABILITY

Both of these tokens were designed to provide the highest levels of quality and reliability in the industry. (For more information on RSA Security's quality process for authenticators, visit [www.rsasecurity.com](http://www.rsasecurity.com) and download the white paper *RSA SecurID Solutions: A Foundation for Enterprise Quality and Reliability*.)

RSA Security has designed and built a full-featured test laboratory to ensure maximum product reliability under demanding, real-world conditions. The company has made a seven-figure investment in this laboratory, which is fully staffed by well-trained reliability engineers. The laboratory includes customized test equipment that reflects challenging real-world conditions.

When RSA Security is designing a new authentication token, a test plan is established to ensure that the authenticator will meet RSA Security's demanding requirements for reliability. The products are tested throughout their life cycle using a rigorous methodology that is well documented. Metrics are carefully captured and tracked on all test conditions, and military sampling levels are exceeded throughout the reliability testing process. Military sampling, which is used by the United States Department of Defense to ensure reliability of the systems it purchases, provides recommended sampling quantities. RSA Security uses these sampling quantities and exceeds them, often by dramatic proportions. By implementing large sample sizes, the laboratory is able to get more accurate statistics on the reliability levels of each lot.

There are no published guidelines for testing tokens, other than the federal requirements with which every token must comply. RSA Security's rich legacy in building highly reliable tokens has enabled a continuous improvement process for both our reliability testing methodology and our reliability testing equipment. The goal of the laboratory is to simulate real-world conditions to make sure that each lot of tokens will survive in the field without incident throughout—and even beyond—its predicted useful life. The testing can be roughly grouped into the following categories:

- Temperature, humidity and altitude;
- Vibration, shock, drop and tumble;
- Electrostatic discharge and
- Ruggedness.

To share insights on the extensive reliability testing performed on lot samples of the RSA SecurID 700 fob token and the RSA SecurID 800 connected authenticator, the following sections provide examples of some of the tests that are regularly conducted to measure reliability levels under the most demanding conditions.

## V. TEMPERATURE, HUMIDITY AND ALTITUDE TESTING

RSA Security's quality assurance testing methodology relies on a large sample size of each lot of these tokens to ensure they will survive the most rigorous temperature, humidity and altitude exposure conditions. The following are some examples of the tests that are conducted.

Reliability tests are conducted under both extreme high-temperature and low-temperature conditions. An example of a high temperature condition might be a user leaving the token in a car parked in the desert. Similarly, that same user might leave the token in a car while visiting Alaska in winter. The reliability laboratory tests token lots at a 65° Celsius (149° Fahrenheit) for a period of 96 hours to ensure that they will survive being left out in extremely high temperature conditions. The same tokens are also tested in a temperature of -20° Celsius (-4° Fahrenheit) for 96 hours to ensure they will survive being left out in the cold.

Temperature cycling conditions are also simulated. For example, a user may leave tokens out under extremely high and low temperatures, such as in a desert where it is very hot during the day but very cold at night. Shock temperature testing simulates both extremes of high temperature and low temperature with a very fast temperature change. This testing also simulates the very fast ascent and descent of an airplane. RSA Security has designed custom test equipment to enable the efficient simulation of these extreme temperatures.

Humidity is another factor that can potentially impact the reliability of a token, so the authenticators are exposed to high humidity tests. Our laboratories conduct tests at 95 percent humidity at a temperature of 35° Celsius (95° Fahrenheit) conditions for 96 consecutive hours, followed by a gradual decrease in temperature and humidity to ambient conditions. This is an important test to ensure the reliability of tokens for users in high-humidity climates, such as in Hawaii or throughout the Asia Pacific.

Since many tokens are likely to be stored at times in cargo bays of airplanes, RSA Security conducts extensive altitude testing. The tokens are placed in a vacuum vessel within an environmental chamber. An altitude of 40,000 feet will be simulated and the temperature will be ramped from ambient temperature to 0° Celsius (32° Fahrenheit) for 12 hours and then to 50° Celsius (122° Fahrenheit) for another 12 hours. This test challenges the token to ensure that it can survive the most challenging altitude conditions of airline travel.

## VI. VIBRATION, SHOCK, DROP AND TUMBLE TESTING

RSA Security conducts extensive, highly customized tests to ensure that these RSA SecurID authentication tokens will survive the most rigorous exposure to vibrations, shocks, drops and tumbles. Mechanical vibration can potentially be a major reason for token failure, so RSA Security conducts vibration testing to ensure that our tokens maintain their structural integrity as they are being vigorously shaken. These tests are conducted to simulate extreme conditions of tokens through conditions such as mail shipments or general handling and travel.

RSA Security conducts vibration tests that include an acceleration of 15 grms with a frequency of 10 to 2000 Hz, with duration of one hour for each of the three axes. After this test, the tokens are visually inspected.

Mechanical shock is another potential problem for tokens. Real-world examples include sudden impact such as if the token is thrown against a wall. RSA Security conducts shock testing to verify that the tokens can survive sudden impact. These tests include a shock of 3500 Gs with a pulse time of .5 ms—and they are conducted on each of the tokens' axes. The tokens are then visually inspected to ensure that they are functioning properly without any damage to the hardware.

Perhaps the most common abuse against a token is when it is dropped. The question is not whether any given token will be dropped during its lifecycle, but rather how many

times it will be dropped and from what heights.

RSA Security conducts extensive drop shock testing to simulate the dropping of the hardware tokens from various heights. Each of these tests is conducted to measure drop shock for each of the axes on a token, and free-form drop tests are also conducted that measure results from drops that do not isolate the impact on a particular axes. The tokens are dropped from 36 inches, 48 inches and from 60 inches to simulate drops, such as from somebody's desk, from somebody's pocket or from a user standing on a ladder or some other high surface. Each of these tests are further measured against different surfaces, including:

- Tiles,
- Rugs and
- Concrete.

Throughout a token's life it will be jarred as it is transported in pockets or purses or banged up against other items as it is put down or put away, so RSA Security conducts extensive tumble testing. These tests are meant to simulate the most extreme real-world conditions. Tokens may even wind up in a dryer when users wash their clothes and inadvertently leave the tokens in the pockets. That is why the laboratory has a custom-designed tumble tester to simulate this jarring impact.

This tumble tester looks like a small clothes dryer. Tokens are placed in this hexagonal tumbling tester along with pocket change and standard keys that a user would likely carry on the same key ring as the token. The tokens then bang against the loose change and the keys as the drum turns for durations of one, two, four and six hours. During these tests, the tokens, coins and keys tumble together and then the tokens are visually inspected to ensure there is no mechanical damage and the token is displaying the correct token code.

## VII. ELECTROSTATIC DISCHARGE TESTING

ESD is the transfer of electrons from one object to another, and it is commonly referred to as static electricity or static shock. Semiconductors are sensitive to ESD, so it is important to test these small, highly intelligent tokens to make sure that they can withstand diverse levels of ESD. All users will expose tokens to ESD by just walking on a rug or playing with a pet. Tokens are tested for both air discharge and surface discharge. Each tested token is "zapped" by an

ESD gun in twenty-six areas at various ESD voltages levels.

Tokens are also commonly stored near radiated immunity fields, such as on a hard drive or on top of a laptop computer. The laboratory tests these tokens for radiated immunity, subjecting them to an 80 percent amplitude modulated radio frequency field to ensure that they can withstand electromagnetic immunity. RSA Security also tests the tokens against X-ray fields that simulate the token passing through an airport's security monitoring system—except the laboratory uses X-ray fields in the simulation that are much stronger than those deployed at airports.

## VIII. RUGGEDNESS CHECKS

RSA Security conducts extensive ruggedness tests to make sure that the tokens will withstand daily use—and abuse. Since both of these tokens are likely to be carried on a ring of keys, tests are conducted to simulate real-world conditions of carrying around the tokens for years. Many users like to play with their key rings. They twirl them, bang them, and even toss them.

A key ring pull-test verifies that the key ring is strong enough to withstand excessive abuse. A customized pull-tester platform performs this test and exerts force until the key ring breaks free of the fob or the connected USB authenticator. Metrics are established in advance to ensure that the force that ultimately breaks the key ring is far in excess of published RSA parameters. A similar test is conducted to measure the force required to separate the post from the plastic housing.

We also implement a key ring rotational wear test to ensure that the key ring can rotate 20,000 revolutions without failure. This simulates more than ten rotations per day for a lifecycle of five years. In addition, force is applied during the rotation to simulate the weight of attached keys.

Perhaps one of the most dramatic checks implemented regularly by RSA Security is the "run over check." This tests whether the token will withstand being driven over a car. The tokens are placed on the pavement and driven over by the car's tire, and then visually inspected to ensure that there is no physical damage and that the correct token code is presented accurately on the display.

Liquids present another ruggedness challenge faced frequently by tokens, so RSA Security conducts immersion testing. In the immersion check, the tokens are dropped into water to ensure that they withstand being soaked. This simulates scenarios such as a token being left in clothes placed into a wash cycle, when a user goes for a swim with the token in a pocket, or perhaps when a token is

accidentally dropped into a drink.

RSA Security also conducts tests that began more informally and are now formalized into the test methodology. For example an RSA Security sales executive often demonstrates the durability of a token by holding the device in his hand then slamming it down on a desk surface. This test has historically often been conducted in customer offices with the RSA Security sales executive challenging a customer to do the same with a token from another manufacturer. This test is now formalized, and the tokens are held face up in the palm of a hand and slammed down onto a desk surface to ensure that each lot sampling will survive the “table slam check.”

The RSA SecurID 800 connected authenticator is subject to additional tests beyond those applied to the fob. For example, since this USB authenticator is frequently inserted into a USB port, a simulation is run to test the authenticator for durability. RSA Security’s USB authenticators are tested to ensure that each authenticator will withstand

#### ESTABLISHING THE MOST DEMANDING METRICS

Like all of the metrics established by the labs, this number was established to measure reliability for the life of a token under extreme usage. This test assumes a user comes to work in the morning and plugs in the connected token, removes it at lunchtime, inserts it again after lunch and removes it at the end of the day. This means the user would insert/remove the device a total of four times per day. If the user worked 250 days per year, that would result in 1,000 insertions/removals. Since the token has a lifecycle of five years, you could extrapolate that the token would be inserted 5,000 times over its useful life. And just to be extra safe, the laboratory decided to double this number and test the token for 10,000 insertions and removals over its useful life.

10,000 insertions—and removals—from a USB port.

The RSA SecurID 800 connected authenticator also comes with a cap to protect the USB connector, so the cap is also tested to ensure that it fits firmly on the RSA SecurID 800

after insertions and removals.

#### IX. CONCLUSIONS

For an enterprise to depend on the broad distribution of tokens to protect access to information and applications, token reliability is a major concern. RSA Security has nearly two decades of experience in designing hardware authenticators and ensuring that they offer the leading reliability levels in the industry.

Anecdotal evidence—while useful—is not enough to ensure that RSA Security continues to hold its leadership in token reliability. The extensive testing conducted in large sample sizes for each lot of tokens provides quantitative proof of the reliability levels of the SecurID authentication tokens. Since RSA Security also tests competitive tokens using these same methodologies, the company can proudly say that RSA SecurID authenticators offer the highest levels of reliability in the industry.

If you would like further evidence, please conduct your own testing using either the methodologies we have described here or ones you develop yourself. For example, if you are evaluating tokens from multiple vendors, perhaps you should take tokens from each vendor and run over them with a car or drop them into a glass of water or a cup of coffee. You could take our tokens and tokens from our competitors and leave them in a trunk of a car in a desert or on a tundra.

RSA Security funds and conducts this extensive testing for one reason; to ensure that customers selecting SecurID solutions can confidently deploy highly reliable tokens that provide the most cost effective management by the enterprise and the most predictable and positive experience for the end user. The enterprise can select tokens from RSA Security, safe in the knowledge that these tokens are highly reliable to withstand the most challenging end-user demands. If you would like more information on our

reliability testing methodology, metrics or results, please contact your RSA sales representative.

#### About RSA Security

RSA Security Inc. helps organizations and individuals confidently protect identities and information access. The company secures more than 15 million user identities, safeguards trillions of business transactions annually, and manages the confidentiality of data in tens of thousands of applications worldwide. RSA Security's portfolio of award-winning solutions—including identity & access management, secure mobile & remote access, secure enterprise access, secure transactions and consumer identity protection—sets the standard in the industry. Our strong reputation is built on a 20-year history of ingenuity, leadership and proven technologies, and our more than 17,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit [www.rsasecurity.com](http://www.rsasecurity.com).

RSA, RSA Security, SecurID and *Confidence Inspired* are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners. ©2005 RSA Security Inc. All rights reserved.

SIDREL WP 0505

