

Vera X512H Unclonable RFID IC

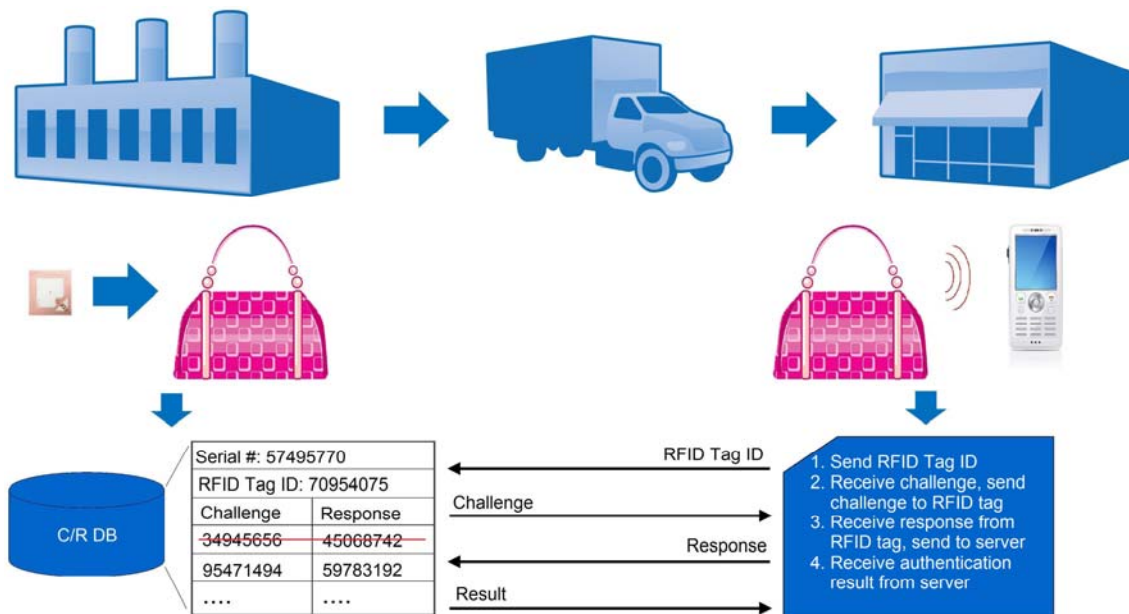
The Vera X512H RFID chips are integrated circuit devices based on Physical Unclonable Functions (PUF) technology. PUF technology makes each and every Vera X512H chip unique and unclonable. Additionally, PUF technology provides a simple, yet strong and robust mechanism to authenticate each Vera X chip. The Vera X chips are based on ISO/IEC 14443-A radio frequency interface, and operate at 13.56 Mhz carrier frequency.

PUF technology is one of the latest breakthroughs in semiconductor security. PUFs are tiny electrical circuit primitives that exploit the unavoidable IC fabrication process variations to generate unlimited number of unique, unpredictable, though reliable “secrets” from each chip. These secrets are dynamically generated, using a challenge response scheme. A PUF is queried with a challenge – a random 64-bit (or longer) number. It almost instantly generates a unique response – a 64-bit (or longer) number. Each PUF can generate a virtually unlimited number of these unique challenge response pairs. Since it is impossible to model or duplicate the IC fabrication process variations, even for the IC manufacturer, it is impossible to generate the same challenge response pairs from another chip. Hence, PUF technology makes ICs effectively unclonable.

PUF generated secrets (challenge response pairs) provide a simple, yet strong and robust authentication mechanism. As shown in the diagram below, a group of challenge response pairs are collected from the chip, and stored in a database. This may usually happen at an initial stage in the life of the chip, perhaps at a secure location. To authenticate the chip at a later time, one of the stored challenges from the database is sent to the chip, the response generated is compared against the one initially recorded in the database. If the two match, the chip is authentic. Since each chip can have multiple challenge response pairs, each challenge response pair is used just once, as a one-time pad. This prevents skimming and replay attacks on PUF authentication.

Highlights

- Unclonable RFID ICs
- Authenticate RFID chips using challenge response scheme
- No skimming and replay attacks – unlimited challenge response pairs, each pair used once
- Based on ISO/IEC 14443-A standard, operating frequency of 13.56 Mhz
- 512 bits of user memory
- Pre-programmed, unique, unalterable 56 bit tag ID
- Anti-collision for simultaneous operations on several chips
- Operating temperature from -25°C to +85 °C
- Operating range up to 10 cm with appropriate antenna





Verayo
Trusted Silicon

The Vera X RFID chips are standard RFID transponders that get activated when an RFID reader sends a request. They have 512 bits of one time programmable read-only memory to store user data. The VERA X1 chips also have a pre-programmed 64-bit tag ID. The Vera X chips support an anti-collision feature to allow simultaneous operations on several chips. The Vera X chip can support PUF challenge and response operation using standard read/write commands, or as custom commands that can easily implemented as an extension to the existing command set of a standard HF 14443-A compatible reader device.

Applications

The Vera X chips enable a secure, robust and cost-effective solution for applications like:

- Anti-counterfeiting
- Secure IDs and access cards
- Electronic ticketing

About Verayo

Verayo delivers a range of security and authentication solutions based on Physical Unclonable Functions (PUF) technology. PUF technology was invented at MIT by Prof. Srinivasa Devadas. Dr. Devadas was joined by Tom Ziola, formerly from Microsoft, to found Verayo in 2005 in Silicon Valley. Verayo is funded by Khosla Ventures and has assembled an experienced Advisory Board drawn from the semiconductor and security industries. The company is currently involved in work for U.S. defense agencies. Verayo is located at 2225 East Bayshore Road, #231, Palo Alto. Email: info@verayo.com. Phone: 650-320-7615. Website: <http://www.verayo.com>.



Verayo