

DIGIPASS PRO 300

Quick Reference

Version 1.0



THE AUTHENTICATION COMPANY

DIGIPASS PRO 300

Quick Reference

Contents

Contents	2
PIN Protection	3
Entering PIN	3
Changing PIN	3
Unlocking Token	3
Response-Only Password	4
Single Application Token	4
Token is Not PIN Protected	4
Token is PIN Protected	4
Multiple Application Token	4
Token Contains Multiple Application	4
Challenge/Response Password	5
Single Application Token	5
Token is Not PIN Protected	5
Token is PIN Protected	5
Multiple Application Token	5
Token Contains Multiple Application	5
Signature Function	6
Single Application Token	6
Token is Not PIN Protected	6
Token is PIN Protected	6
Multiple Application Token	6
Token Contains Multiple Application	6

PIN Protection

A PIN is a 4 to 8 digit that is used to guard against the unauthorized use of the token. Once the token is PIN protected, a correct PIN entry is **required** to activate the token.

Entering PIN

If the Digipass Pro 300 token is PIN protected, you must enter the correct PIN in order for it to become operational.

1. Press the ◀ button to turn the power on.
2. At the “PIN” prompt, enter the PIN.
3. If the wrong PIN is entered and the “FAIL #” is displayed, simply press the ◀ button to restart. *Warning: Token will **lock** upon too many consecutive invalid PIN attempts.*

Changing PIN

The Digipass Pro 300 token must be pre-configured during initialization to allow the user to change the PIN.

1. Press and hold the ◀ button until “NEW PIN” is displayed.
2. Enter the new PIN until “PIN CONF” is displayed.
3. Enter the new PIN again until “NEW PIN CONF” is displayed.
4. If the PIN confirmation fails, the “FAIL” message is displayed and steps 2 and 3 needs to be repeated.

Unlocking Token

The Digipass Pro 300 token becomes inoperable (LOCKed) if too many consecutive invalid PIN entries are attempted, the usage time-limit has been reached, the usage count-limit has been reached, or the battery is low in power.

Once the Digipass Pro 300 token is locked, it must be unlocked before it can be used. The Digipass Pro 300 token uses unique inverse challenge/response processing to unlock the token.

Each implementation of the Digipass Pro 300 token may adopt different procedures on unlocking the token, but generally, a token user would call up the help desk with the lock-value that is displayed on the token and the help desk personnel would issue the unlock-code after verifying the user’s identity.

Please consult your company’s procedure on unlocking Digipass Pro 300 tokens.

Response-Only Password

Response-Only mode requires *no* input data to generate the dynamic password.

Single Application Token

These tokens can only operate in a response-only password function.

Token is Not PIN Protected

1. Press the ◀ button to turn the power on and to generate the one-time password.

Token is PIN Protected

1. Press the ◀ button to turn the power on.
2. Enter the PIN to generate the one-time password.

Multiple Application Token

These tokens contain a combination of challenge/response password, response-only password, and signature functions.

Token Contains Multiple Application

1. Press the ◀ button to turn the power on.
2. Enter the PIN. (If PIN is prompted)
3. Press **1**, **2**, or **3** to select the response-only application and to generate the one-time password.

Challenge/Response Password

Challenge/Response mode *requires an input challenge data* issued by the security/host server (such as Vacman Server) to generate the dynamic password.

Single Application Token

These tokens can only operate in a challenge/response password function.

Token is Not PIN Protected

1. Press the ◀ button to turn the power on.
2. Enter the challenge data to generate the one-time password.

Token is PIN Protected

1. Press the ◀ button to turn the power on.
2. Enter the PIN.
3. Enter the challenge data to generate the one-time password.

Multiple Application Token

These tokens contain a combination of challenge/response password, response-only password, and signature functions.

Token Contains Multiple Application

1. Press the ◀ button to turn the power on.
2. Enter the PIN. (If PIN is prompted)
3. Press **1**, **2**, or **3** to select the challenge/response application.
4. Enter the challenge to generate the one-time password.

Signature Function

Signature mode *requires one or more input data* to generate the signature.

Single Application Token

These tokens can only operate in a signature function.

Token is Not PIN Protected

1. Press the **◀** button to turn the power on.
2. Enter the input data.
3. Repeat step 2. while entering new data each time until the signature is generated.

Token is PIN Protected

1. Press the **◀** button to turn the power on.
2. Enter the PIN.
3. Enter the input data.
4. Repeat step 3. while entering new data each time until the signature is generated.

Multiple Application Token

These tokens contain a combination of challenge/response password, response-only password, and signature functions.

Token Contains Multiple Application

1. Press the **◀** button to turn the power on.
2. Enter the PIN. (If PIN is prompted)
3. Press **1**, **2**, or **3** to select the signature application.
4. Enter the input data.
5. Repeat step 4. while entering new data each time until the signature is generated.