

A Total Cost of Ownership Analysis
On
Strong Authentication with One Time Passwords



1 Setting the scene - What is strong authentication

Authentication is the process of identifying entities and this process can be assisted by a number of different tools which helps prove the identity. In the physical world this process is often carried out using either a possession of a physical proof as a key or passport or it can be something you know as an access code or bank account number.

Authentication in the digital world is used to map a physical identity (even though it might be digital as an application) to a digital identity as when Joe Doe the person logs on to the network using his user id in the network. How the entity authenticates depends on what kind of method the system the entity authenticates to requires. In the digital world authentication is grouped into several different groups and names as password authentication, two factor authentication, PKI authentication etc, but it all comes down to two main groups one factor or two factor authentication.

One factor authentication solutions is when the user only has to prove knowledge or possession of something. Typically this is when the user authenticates using a username and password or a USB token that does not requires additional authentication.

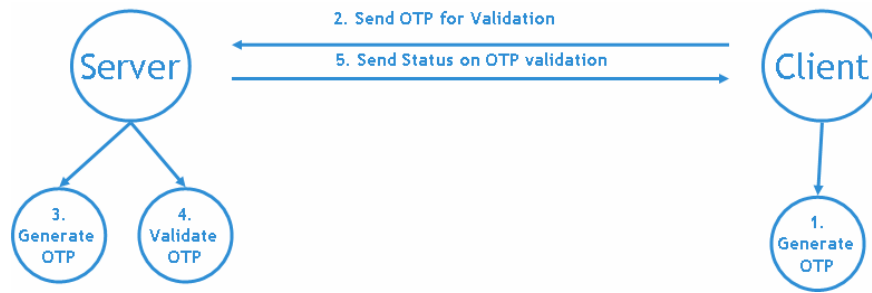
Two factor authentication require a combination of knowledge and possession i.e. something the entity knows and something the entity possess.

Strong authentication is a two factor solution where knowledge and possession is combined in the same solution. There are sub-groups within strong two factor authentication but in this document we will concentrate on the mostly spread one - Strong Two Factor Authentication using One Time Passwords (OTP).

1.1 What is an OTP?

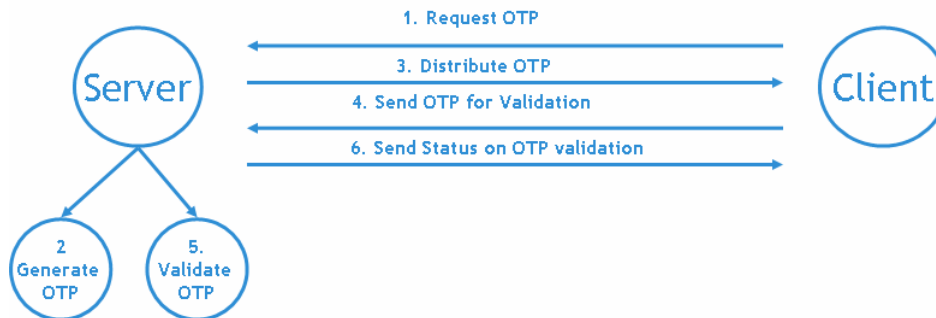
A One Time Password (OTP) is, as the name indicates, a password that can only be used once. The basics are that there is a server and a client. There are then two main options how the OTP is generated, distributed and validated.

The first option is that the server and the client share a common shared secret and a cryptographic algorithm and these are then used to generate a OTP at both ends. If the server validates the two OTP's to be the same the authentication is successful.



Option 1

The other option is that the server generates the OTP and distributes it to the client in a secure manor. The client then submits the OTP back to the server and if the server validates the two OTP's to be the same the authentication is successful.



Option 2

2 *The OTP market offerings*

The market for OTP's have up until now been dominated by solutions built upon use of separate hardware authenticators that generate OTPs either on-demand or using a timer. Some of the solutions have a validity time others are restricted by the length of the battery life-time. Even though widely deployed these solutions all share several issues ranging from cost issues to usability issues as;

- Tokens are expensive to deploy, distribute, own and manage
- Users forget the tokens
- Users loose the tokens
- Users find tokens difficult to use

2.1 *The PortWise offering*

PortWise offers strong authentication with use of One Time Passwords without the limitations solutions based on authenticators have. The PortWise Secure Application Access Platform offers a solution where users can use existing hardware as the possession part in two factor authentication. With innovating software PortWise is able to make use of the existing hardware and combine it with the knowledge part and give users strong authentication using OTPs and at the same time offer highest usability and cuts costs giving almost an instant ROI.

Administrators can select to deploy both types of options, described earlier in this document, depending on what best suites the problem they are trying to solve, they might even offer the user to select the type to use. The solution consists of a server part and different types of clients. These clients are;

- PortWise Mobile ID for Pocket PC (option 1 type)
- PortWise Mobile ID for Palm (option 1 type)
- PortWise Mobile ID for Java enabled Mobile Phones (option 1 type)
- PortWise Mobile ID for Windows Mobile (option 1 type)
- PortWise Mobile ID for Windows (option 1 type)
- PortWise Mobile ID Mobile Text (option 2 type)
- PortWise Mobile ID Web (a one factor authentication method)

All of the option 1 types can be used in two different modes, **synchronized** and **challenge**.

With **challenge** mode the user is required to sign a text that the system has asked the users to sign. This enables use of digital signatures. Once the user has entered the challenge the OTP is generated. **Synchronized** mode does not require the use of a challenge instead the user only enters the pin and then the OTP is generated.

PortWise Mobile ID Mobile Text distributes the server generated OTP to the client using the mobile text network and requires no client on the cellular phone.

PortWise Mobile ID clients can be distributed using the PortWise Distribution Server which is an automated service that also assists users in configuring the PortWise Mobile ID client.

To further reduce administration costs PortWise Authentication Service is fully integrated with leading user storages as Microsoft Active Directory, Novell eDirectory and Sun Java Directory Server. By leveraging this integration auto-enrollment of users is possible which then means there is no end user management.

The PortWise Authentication Service is easily enabled at applications using RADIUS or the web service interface available at the PortWise Authentication Service server.

2.2 *Feature comparison of vendors in this TCO comparison*

Feature	PortWise	RSA	Secure Computing
Supports RADIUS	Yes	Yes	Yes
Provides Web Services Interface	Yes	No	No
Supports Auto enrollment of users	Yes	No ¹⁾	No ¹⁾
Supports digital signatures	Yes	No	No
Supports LDAP Connectivity through tight integration	Yes	No	No
Supports use of mutual directory servers	Yes	No	No
Requires dedicated database	No	Yes	Yes

¹⁾ Self service enrollment available as add-on

3 Total Cost of Ownership Comparison

3.1 Setting the scene - OTP Inc

OTP Inc, a company of 5,000 employees worldwide manufactures products for the consumer market. The company has many users travel and has recently started a flexible working program in which the company encourages employees to work out of office. The company also has 3,500 partners worldwide who all shall have access to the extranet. The authentication service shall be placed at a central point in the network and be integrated with Active Directory for the corporate users and with Sun Java Directory Server for the extranet users.

Out of the 5,000 employees 4,000 needs to be provided with an OTP based authentication solution. Of these 4,000 employees 3,700 works in other offices at other locations than the headquarters in OTP Valley. Along with the partners the requirement adds up to 7,500 users. If a separate hardware token is to be used 7,200 users of the 7,500 total needs to have the token shipped to them.

3.2 Calculations

NOTE: All prices in this calculation are list prices. Discounts are not taken into account.

3.2.1 Per user costs

Cost	PortWise	RSA	Secure Computing
Cost per user	\$90	\$116 ²⁾	\$109
Average shipping cost per unit ⁴⁾	\$0	\$5	\$5
Enrollment cost	\$0 ¹⁾	\$10	\$10

Note

- ¹⁾ Users are enrollment automatically using their existing directory password
- ²⁾ Tokens are valid for 36 months
- ³⁾ OTP Vendor 1 and OTP Vendor 2 do not support use of mutual directories and in real would require separate servers to support the OTP Inc environment.
- ⁴⁾ Hardware tokens needs to be shipped to the user.

3.2.2 Cost for 7,500 user deployment

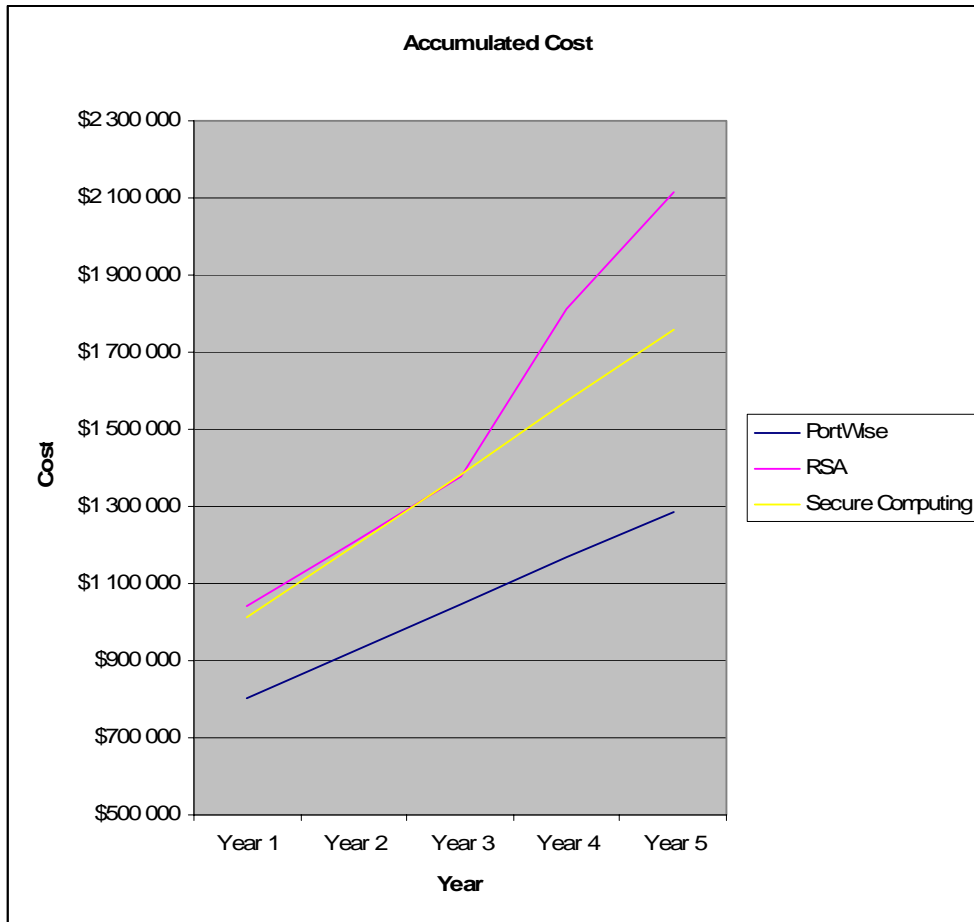
Cost	PortWise	RSA	Secure Computing
License	\$675 000	\$868 500	\$819 813
Server (to run on)	\$ 5 000	\$ 5 000	\$5 000
Maintenance and Support contract	\$121 500	\$43 393	\$88 594
Annual replacement ¹⁾	0\$	\$124 740	\$97 969
Total Year 1	\$ 801 500	\$1 041 633	\$1 011 376

- ¹⁾ Surveys indicate that between 15%-30% of all tokens are damaged, broken or lost during a year. This calculation estimates 20%.

3.2.3 Five year cost stream

Vendor	Year 1	Year 2	Year 3	Year 4	Year 5	Accumulated
PortWise	\$801 500	\$121 500	\$121 500	\$121 500	\$121 500	\$1 287 500
RSA	\$1 041 133	\$168 133	\$168 133	\$434 220 ¹⁾	\$303 840	\$2 135 459
Secure Computing	\$1 011 376	\$186 563	\$186 563	\$186 563	\$186 563	\$1 757 628

1) 60% of the tokens have been replaced as lost in year 1, 2 and 3. 40% is replaced in year 4 and in Year 5 as the validity time for the token is 36 months.



3.2.4 Savings

OTP Inc will save

- \$827 959 or 39% over a 5 year period if they deploy PortWise instead of RSA
- \$470 128 or 27% if they deploy PortWise instead of Secure Computing

The savings calculation excludes things as;

- Reduced production loss if a token is lost
- Reduced production loss if a token is forgotten
- No hassle for partners with additional tokens

4 Cost Balance Sheets

This chapter shows the costs for implementing and owning a OTP strong authentication solution over three years.

4.1 Cost for a 1,000 user deployment

	PortWise	RSA SecurID	Secure Computing Safeword
License Cost	\$90 000	\$136 094	\$133 184
Maintenance 3 years	\$48 600	\$34 939	\$52 163
Token Distribution Costs	\$0	\$5 000	\$5 000
Token Replacement ²⁾	\$0	\$42 187	\$40 500
Enrollment Cost ¹⁾	\$0	\$10 000	\$10 000
TOTALS	\$138 600	\$228 220	\$240 847
Save \$ with PortWise		\$89 620	\$102 247
Save % with PortWise		39%	43%

¹⁾ Enrollment costs include tasks when setting up the user. PortWise offers an automated enrollment.

²⁾ Research shows that somewhere between 15-30% of the deployed are lost or broken during on year. In the above table a value of 20% has been used.

4.2 *Cost for a 500 user deployment*

	PortWise	RSA SecurID	Secure Computing Safeword
License Cost	\$45 000	\$77 107	\$65 825
Maintenance 3 years	\$24 300	\$22 173	\$52 163
Token Distribution Costs	\$0	\$2 500	\$2 500
Token Replacement ²⁾	\$0	\$21 431	\$17 250
Enrollment Cost ¹⁾	\$0	\$5 000	\$5 000
TOTALS	\$69 300	\$128 210	\$119 195
Save \$ with PortWise		\$58 910	\$49 895
Save % with PortWise		46%	42%

¹⁾ Enrollment costs include tasks when setting up the user. PortWise offers an automated enrollment.

²⁾ Research shows that somewhere between 15-30% of the deployed are lost or broken during on year. In the above table a value of 20% has been used.

4.3 Cost for a 100 user deployment

	PortWise	RSA SecurID	Secure Computing Safeword
License Cost	\$9 000	\$22 109	\$17 585
Maintenance 3 years	\$4 860	\$7 926	\$10 125
Token Distribution Costs	\$0	\$500	\$500
Token Replacement ²⁾	\$0	\$4 388	\$3 525
Enrollment Cost ¹⁾	\$0	\$1 000	\$1 000
TOTALS	\$13 860	\$35 922	\$31 235
Save \$ with PortWise		\$22 062	\$17 375
Save % with PortWise		61%	56%

¹⁾ Enrollment costs include tasks when setting up the user. PortWise offers an automated enrollment.

²⁾ Research shows that somewhere between 15-30% of the deployed are lost or broken during on year. In the above table a value of 20% has been used.