



Dave Cummings
Chief Information Officer

Technology Services

121 Library Court Oregon City, OR 97045

Board of County Commissioners
Clackamas County

Members of the Board:

Approval to Purchase SecureAuth Subscription for Identity/Access Management and Multifactor Authentication

Purpose/Outcomes	Provides tools to enable secure authentication and identity management for remote access, cloud applications, internal services, and more to prevent unauthorized access to County resources and meet security compliance requirements for CJIS , HIPAA, etc.
Dollar Amount and Fiscal Impact	\$56,116.94 - Annual Payment in FY20-21 \$56,116.94 - Annual Payment in FY21-22 \$56,116.94 - Annual Payment in FY22-23 ----- \$168,350.82 Total Contract over 3 years from SHI
Funding Source	Existing Technology Services Allocated budget. Specifically 747-0227 capital fund.
Duration	3 years
Previous Board Action	none
Strategic Plan Alignment	Direct support for County and Technology Service initiatives for: <ul style="list-style-type: none"> - Build a strong infrastructure - Build public trust through good government
Counsel Review	Counsel reviewed/approved transaction method on 3-3-21
Contact Person	Dave Devore (503) 723-4996

BACKGROUND:

Clackamas County Technology Services (CCTS) has recognized the need to enable multifactor logons for remote access, cloud hosted applications, and any application or service needing to meet compliance requirements for CJIS, HIPAA, or other similar rulesets

The existing practice of relying solely on username and password for remote access has proven ineffective and has resulted in multiple unauthorized logon events via phishing attacks to users. The recent changes during the Covid crisis response with more users working remotely has further exacerbated the issue. Additionally, we have been noted in multiple audits in recent years due to our weak password policy and lack of mandatory multi factor authentication for users with CJIS or other compliance requirements. From a security perspective, this project is long over-due.

After reviewing the leading solutions, CCTS has concluded that the County would be best served by SecureAuth, which provides the best balance of features, support, and price. A more detailed proposal document is available upon request.

Funds for this Agreement are budgeted in the Technology Services budget in Fund 747 Program 227 Account 485320. TS will continue to budget funds for the duration of this agreement through FY21-22 and FY22-23.

PROCUREMENT PROCESS

Technology Services staff obtained three quotes from vendors for the exact same service quantities. The quotes ranged \$302,400.00 to \$168,350.82. The lowest cost quote is under contract that meets the requirements of Permissive Cooperative Procurements under LCRB Rule C-046-0430. By obtaining multiple quotes and taking advantage of a special pricing offer under a cooperative contract, Technology Services was able to realize substantial cost savings for the County. County Counsel has reviewed and approved the cooperative contract and this transaction.

RECOMMENDATION:

Staff respectfully recommends approval of the renewal of the SecureAuth subscription through SHI. Staff further recommends that the Board delegate authority to the Technology Services Director to sign agreements necessary in the ongoing performance of this agreement.

Sincerely,



David Cummings, CIO
Director, Clackamas County Technology Services

Placed on the _____ agenda by Procurement



CLACKAMAS
C O U N T Y

Technology Services
Enterprise MFA Proposal
2021

Table of Contents

1. Overview	2
2. History.....	2
3. Goals.....	2
3.1. Security Remote Access.....	2
3.2. Integration with County and vendor provided apps	2
3.3. Broad Set of Authentication factors.....	2
3.4. Adaptive Technology	3
3.5. Additional features considered	3
4. Technology Overview	3
4.1. Identity and Access Management.....	3
4.2. Multifactor Authentication	3
4.3. Adaptive Authentication.....	4
5. Solution comparison.....	4
5.1. Solution Summary.....	4
5.2. Matrix	4
5.3. Matrix Conclusion	5
6. Solution Summary	6
6.1. Secure Auth General Design.....	6
6.2. SecureAuth Integration.....	6
6.3. Secure Auth Available Factors	7
6.4. SecureAuth Adaptive Authentication.....	7
6.5. Cost.....	8
7. Conclusion	8
8. References	9
8.1. General overview references.....	9
8.2. SecureAuth product references.....	9
8.3. Customer Case Studies	9

1. Overview

Clackamas County Technology Services (CCTS) has recognized the need to enable multifactor logons for remote access, cloud hosted applications, and any application or service needing to meet compliance requirements for CJIS, HIPAA, or other similar rulesets. The intent of this document is to provide an overview of the new design as well as insight into the factors that have led us to choose this design strategy.

2. History

The existing practice of relying solely on username and password for remote access has proven ineffective and has resulted in multiple data breaches via phishing attacks to users. The recent change to stop password rotation during the Covid crisis response has further exacerbated the issue. Additionally, we have failed multiple audits in recent years due to our weak password policy and lack of multi factor authentication for users with CJIS or other compliance requirements.

3. Goals

For the next generation of the County's remote access authentication, CCTS has considered several technology goals in our aim to modernize the authentication process with consideration to existing systems and integration to public cloud infrastructure.

3.1. Security Remote Access

The selected solution needs to be flexible enough to accommodate existing infrastructure. Integration with existing remote access solutions such as the Pulse SSL, Citrix Netscaler, or other solutions as identified is required. The primary function for this project is to secure remote access connectivity for users.

3.2. Integration with County and vendor provided apps

There are a number of first and third party applications that would benefit, or may require, additional security. The selected solution should have the flexibility to integrate with applications both on-premise and cloud hosted.

3.3. Broad Set of Authentication factors

Multiple methods for identity verification should be provided. App enrollment, one time passwords over SMS or email, static pin, Oath token, yubikey, telephony and others are examples of the various

ways MFA can be achieved. The preferred solution will provide a wide array of options to accommodate current and future authentication requirements.

3.4. Adaptive Technology

The MFA solution should be adaptive, or contextually aware, such that it allows for automated adjustments to the authentication requirements (increasing or decreasing) under certain conditions based on dynamically monitored risk factors (such as location, source device, destination, account behavior, etc).

3.5. Additional features considered

While not priority requirements, some MFA solutions allow for additional features such as identity management, application portals, and self-service tools for users.

4. Technology Overview

4.1. Identity and Access Management

Identity and access management, or IAM, is the security discipline that makes it possible for the right entities (people or things) to use the right resources (applications or data) when they need to, without interference, using the devices they want to use. IAM is comprised of the systems and processes that allow IT administrators to assign a single digital identity to each entity, authenticate them when they log in, authorize them to access specified resources, and monitor and manage those identities throughout their lifecycle. <https://www.ibm.com/topics/identity-access-management>

Many of the Enterprise MFA solutions are also identity solutions that also provide for securing authentication. They often provide their own identity engine, a duplicate set of our AD user accounts as an example, from which they can tightly integrate with systems, present applications in a portal and deliver workflow for systems and application access.

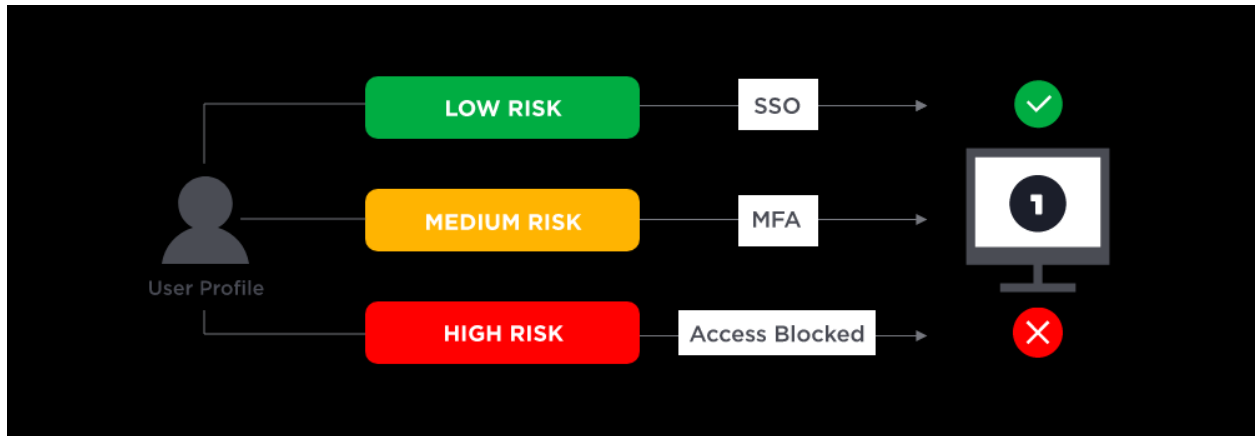
4.2. Multifactor Authentication

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

<https://www.onelogin.com/learn/what-is-mfa>

4.3. Adaptive Authentication

Also called risk-based authentication, is a process where the factors required for authentication vary depending on risk conditions. Adaptive authentication systems use analytics to dynamically review the user properties, destination, location, device, and other criteria, in real time during the authentication process and adjust the level of security required (including denying access). These systems work through a combination of pre-defines policies and real time contextual intelligence processing.



5. Solution comparison

5.1. Solution Summary

Given the goals outlined in section 3, we reviewed multiple top tier solutions in the MFA and identity space. The comparison and notes in the matrix below represent the top solutions compared and is not exhaustive of all of the solutions considered.

5.2. Matrix

	Duo	Okta	SecureAuth	Microsoft
Security 3.1	Meets all primary security concerns for Remote Access and M365.	Meets all primary security concerns for Remote Access and M365.	Meets all primary security concerns for Remote Access and M365.	Meets all primary security concerns for Remote Access and M365.
Integration 3.2	Most robust and wide-reaching native integration in the industry. Easiest deployment. Has API available for specialty	Integration with most commercial apps. Has API available. Builds portal to present applications. Strong integration with Microsoft services.	Fewer native integrations. Relies more on API and custom workflow. Highly flexible but more work up front.	Microsoft focused. Integration with other cloud services okay. On prem integration is either challenging or not

	apps. Compatible with pretty much anything.	Represents shift in how apps are presented.		possible depending on specifics.
Broad Auth Factors 3.3	Meets/exceeds expectations	Meets/exceeds expectations	Meets/exceeds expectations	Limited to fewer options
Adaptive 3.4	Yes	Yes	Yes	Yes, but least feature rich. Even at higher licensing level.
Other features 3.5	Most widely used and supported.	Is full identity engine with universal directory for user profiles. Can service county users and citizens. Has other tools like password self-service.	Has suite of password management tools for unlock, reset, etc. Supports password-less authentication.	None of note.
Cost 3.6	Second most expensive. ~100k per year	Most expensive. More than 100k per year.	Third most expensive. ~60k annually.	Least expensive. Included with current Enterprise Agreement.
Final	☹ Solid solution and feature rich. Most used across industry but comes at premium price. Shifting to become more identity management based like Okta.	☹ Given unlimited time and budget this would be our preferred solution. Especially if we were wanting a full identity management solution. Price and scope is simply too big for our current needs.	☹ Exceeds our requirements and is focused on security and MFA. Seems to be best fit and best value.	☹ Already owned but unfortunately cannot meet our current needs.

5.3. Matrix Conclusion

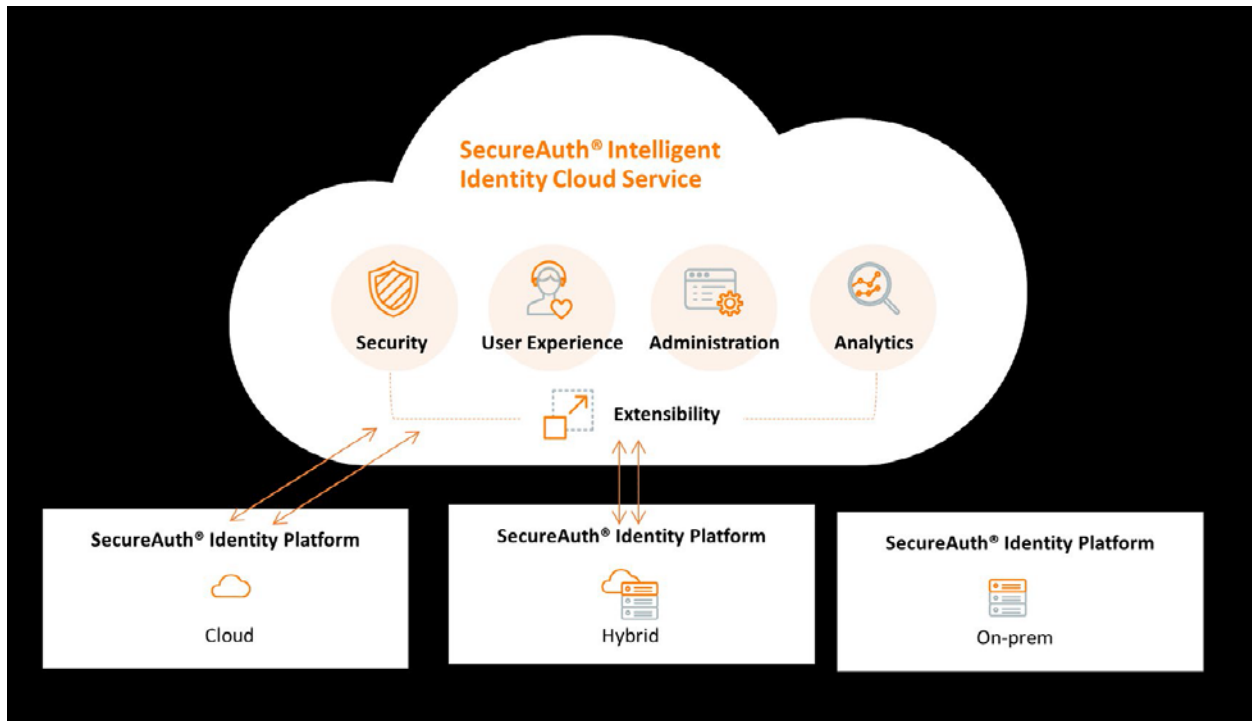
Okta and Duo are the heavy hitters in the industry. They used to be companion apps with Duo providing MFA and Okta providing identity management. They now compete more directly as they build their solutions to match feature sets. This makes both solutions very powerful but ultimately also makes the deployment much broader in scope and more expensive.

Microsoft’s limited support for on premise applications makes it a non-starter even though we own it already. Additional solutions were reviewed and discussed but were dismissed on technical, cost, or other considerations.

After reviewing the best solutions available, we’ve concluded that the County would be best served by a solution targeted specifically towards MFA instead of investing into an identity managing platform at this time. Using this approach reduces complexity, cost, and more quickly solves the immediate security concerns. For these reasons, SecureAuth represents the best choice and is our recommendation.

6. Solution Summary

6.1. Secure Auth General Design



6.2. SecureAuth Integration


(From Tech Target) SecureAuth IdP comes from the SSO world and, as such, reflects a very strong federation and [Security Assertion Markup Language \(SAML\)](#) story. This means the MFA product is easily integrated into a wide variety of applications, and under an assortment of circumstances, especially as SAML gains credence and popularity among SaaS applications.

Besides SAML, SecureAuth IdP can leverage a number of other MFA integration methods. These include, for example, specific agents that customers can add to Microsoft Internet Information Services, Apache Tomcat and JBoss web servers to enable those technologies to accept the authentication federation. It also supports virtually all [VPNs](#) currently on the market, any application that supports federation and any application where the customer controls the login page itself. All of this makes SecureAuth IdP a very flexible, strong authentication tool.

<https://searchsecurity.techtarget.com/feature/Multifactor-authentication-products-SecureAuth-IdP-v80>

<https://docs.secureauth.com/display/SIWA/SAML+Application+integration>

6.3. Secure Auth Available Factors


Admin ▼

Multi-Factor Methods

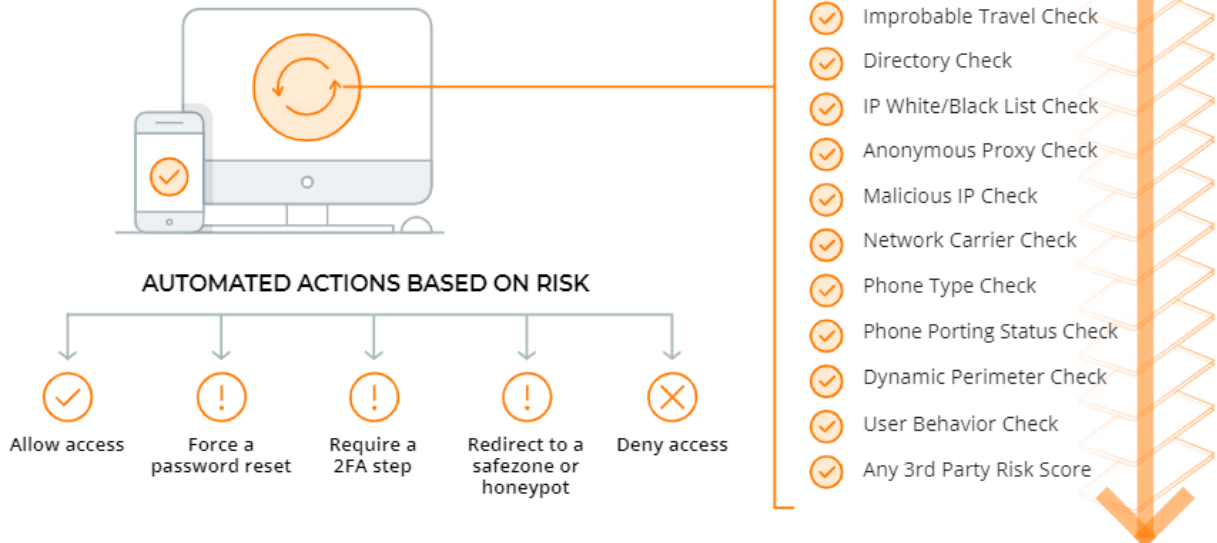
Enable and configure the methods available for use by your organization.

Method configuration

TYPE	STATUS	CONFIGURATION MODE	✎
FIDO2 (WebAuthn)	● Enabled	✔ FIDO2 Devices	✎
YubiKey	● Enabled	✔ OATH HOTP ✔ Yubico OTP	✎
Authentication Apps	● Enabled	✔ One-time passcode ✔ Timed passcode from app ✔ Biometric identification ✔ Login notification	✎
Text Message	● Enabled	✔ One-time passcode ✔ Login confirmation link	✎
Email	● Enabled	✔ One-time passcode ✔ Login confirmation link	✎
Voice Phone Call	● Enabled	✔ One-time passcode	✎
Security Questions	● Enabled	✔ Security questions	✎
PIN	● Enabled	✔ Personal identification number	✎
Symantec VIP	● Enabled	✔ Timed passcode	✎

6.4. SecureAuth Adaptive Authentication

SECUREAUTH ADAPTIVE AUTHENTICATION –
BETTER SECURITY & BETTER USER EXPERIENCES



6.5. Cost

Listed below are the total project costs based on best quoted price as of 12/31/20. Current quoted price is based on three year contract (paid annually).

- 1) IdP - PROTECT - Unlimited Apps- Year 1
 - a. SecureAuth - Part#: IdP – PRO
 - b. Coverage Term: 12/17/2020 – 12/16/2021
 - c. **Note:** 12 months- per user pricing for annual subscription
 - d. **Quantity** 2500 @ \$19.35
 - e. **Sub Total** \$48,375.00
- 2) SecureAuth IdP virtual appliance on Windows- Year 1
 - a. SecureAuth - Part#: VM-Windows
 - b. Coverage Term: 12/17/2020 – 12/16/2021
 - c. **Note:** 12 months- production VM appliance license for a year
 - d. **Quantity** 2 @ \$3,870.97
 - e. **Sub Total** \$7,741.94
- 3) SecureAuth IdP DEV/NFR virtual appliance on Windows- Year 1
 - a. SecureAuth - Part#: VM-Windows-DEV
 - b. Coverage Term: 12/17/2020 – 12/16/2021
 - c. **Note:** 12 months- Dev VM appliance license for a year
 - d. **Quantity** 1 @ \$0.00
 - e. **Sub Total** \$0.00
- 4) **Totals**
 - a. Per Year: \$56,116.94
 - b. Three Yr TCO: \$168,350.82

7. Conclusion

We firmly believe that SecureAuth is the best Adaptive MFA solution to meet the security, functionality, and regulatory compliance challenges for authentication in the coming years. It is the only solution that best balances our project goals, available features, scalability for future growth, and cost.

This document cannot cover all of the details of the technical review process, but it is our hope that we have made the case as to why the proposed design and the associated vendor(s) were selected. We are eager to discuss the proposal in further detail and we are excited to be able have the opportunity to move forward with this project.

8. References

8.1. General overview references

<https://www.onelogin.com/learn/what-is-mfa>

<https://www.centrify.com/blog/what-is-adaptive-authentication/>

<https://www.ibm.com/topics/identity-access-management>

8.2. SecureAuth product references

<https://www.secureauth.com/identity-access-management/multi-factor-authentication/>

<https://www.secureauth.com/identity-access-management/adaptive-authentication/>

<https://www.secureauth.com/identity-access-management/user-lifecycle-management/>

<https://www.secureauth.com/identity-access-management/risk-engine-service/>

<https://searchsecurity.techtarget.com/feature/Multifactor-authentication-products-SecureAuth-IdP-v80>

8.3. Customer Case Studies

<https://www.secureauth.com/customers/>

<https://www.secureauth.com/resource-center/>

<https://www.featuredcustomers.com/vendor/secureauth/case-studies>