# University of Colorado Multifactor authentication for HR self-service

In 2014, the University of Colorado went through a process of deploying a step-up, multi-factor authentication for sensitive components of their employee self-service portal. The entire effort, from initial concept to production go-live, was within six months; including requirements gathering, selection of method and technology, implementation, testing, communications and launch. This paper describes the process, key decisions and lessons learned through the project and in several months of usage.

## Motivation, requirements and selection

The project was initiated following a round of direct deposit payroll fraud originating from email phishing targeted at one of the CU campuses. A number of people fell victim and their pay was redirected to a different bank account. As part of the response to this incident, the self-service direct deposit function was taken offline until improved security controls could be put into place. In the meantime, changes were processed via paper forms. (Note: the self-service system already provided an email notification of changes to the employee. It is unclear if the employees ignored these notifications of if the attacker deleted them before the employee saw them.) A number of options were discussed and below is a brief summary of some of the rationale for eliminating those options:

* Restrict access to on-campus, including VPN– attackers demonstrated use of VPN services, so this was not an effective mitigation
* Restrict access to on-campus, excluding VPN – We have employees who do not work on the campuses and the desire was to have equal functionality for these employees.
* Require a manual approval step for all, or a higher risk subset, of changes to direct deposit – with 30,000+ employees, this is a frequently used function and the changes are sometimes time critical. It was also unclear how to best vet the change requests – requiring manual confirmation of the change outside of the self-service portal could be labor intensive.
* Perform multi-factor authentication using an existing piece of information we know about the person – we could not identify a piece of information that both existed for all employee records and would not be accessible to an attacker who had access to the victim’s email
* Collect new information from the employees to be used for MFA (e.g. security questions or a PIN) – This would require a challenging process of getting all employees to provide this information, or assigning information and distributing it (PIN). Plus it would need additional self-service and support paths.
* Expanded phishing awareness/training efforts – this was a separate effort that was already underway, but the incident reinforced the risks associated with phishing.
* Use a third-party information-based MFA (like RSA risk based authentication) – These options appeared to be fairly heavy-weight to implement and the user experience was not judged as good (asking questions that the user might have to go digging for an answer).
* Use a third-party phone-based authentication – We ultimately selected this route, but needed an option that supported voice and SMS because not all users would have smart phones.

We focused on the last two options and had conversations with both vendors and peers about different products in the two spaces. Ease of implementation and user experience were the largest issues with the information-based systems like RSA and Oracle OAAM. However, they did have the advantage of making more dynamic decisions based on the context (source IP, computer, etc.). Some of the phone-based options (like Google Authenticator) required a smartphone, which wasn’t a reasonable requirement for our broad user base. Some were SMS-only and we wanted to support the ability to call land-lines for those without a cell phone or who had per-message charges on their cell phone. The combination of flexible implementation options and good discounts for higher education via InCommon made the Duo offering appealing and it quickly became a the front-runner.

Key requirements:

* Successfully mitigates common phishing attacks
* Easy for end users – these functions are used infrequently (maybe twice a year by a given individual), so we can’t rely on a learning curve
	+ Works for all employees – shouldn’t prevent self-service based on location, type of device, etc.
	+ Should not be overly complicated to complete additional verification
	+ Minimal disruption of work – since the sensitive/critical functions were infrequently used, we focused on solutions where we would only require MFA for those pieces and not for every login.
* Rapid deployment – desired timeline of no more than six months

## Key decisions

One of our early decisions was to use GreyHeller ERP Firewall as the mechanism to decide when to invoke multi-factor authentications. This product is an add-on to the existing PeopleSoft web (PIA) servers that allows for additional access control and logging decisions. There were multiple reasons for this choosing this option, including ERP Firewall’s ability to make decisions based on PeopleSoft data like user role (for future privileged user MFA), the ability to leverage other features of ERP Firewall (like enhanced logging) and an existing higher education customer using the PeopleSoft/ERP Firewall/Duo combination.

We discussed multiple models for populating phone number data into Duo. We selected to build a real-time integration from the HR system (PeopleSoft) to Duo via our standard middleware (Oracle Service Bus and Master Data Management). This gave us a substantial base of data to work from, but the data was expected to be outdated and/or incomplete in many cases. To address this issue, we did a communication campaign about updating employee contact numbers combined with pop-up at login for the HR self-service portal (showing their current numbers and forcing them to acknowledge or update them). More than 20,000 employees either acknowledged their current numbers as accurate or updated their phone numbers prior to launch, although we still had a small portion of users with no phone numbers in HR. This gave our Employee Services department the added bonus of higher data quality in the HR system. We chose to populate Duo with home, office and mobile numbers from HR. While some office numbers are shared by multiple people, the goal of the control is mitigating external attacks, not attacks from people within the same office.

Given the large user base (34,000) with very infrequent use (2-3 times a year), we chose to only support voice and SMS based authentications for this use case. Using the smartphone app required a registration step and the vendor did not supply a self-service function at the time. With large user bases and short smartphone life (~20 months), re-registering new phones becomes a frequent event and a potential support issue. It also didn’t seem efficient to install a mobile app would only be used 2-3 times a year. Multiple other institutions expressed concern about the telephony costs for a non-app based deployment. One can readily do the math on the number of times the multifactor would be invoked and the cost per message. Our estimate came in at under $2000 per year, much smaller than the licensing costs for the software.

In working with Employee Services (our key stakeholder), we chose a support model that directed users to first contact Employee Services with questions/problems, then issues could be escalated to IT. One of the main reasons for this model was the expectation (which has proven true) that most calls would be about incorrect phone numbers. Because we planned to use a real-time integration, fixes to phone numbers needed to be made in the HR system and would automatically propagate to Duo.

Another factor in our process was the desire to select and build a technology that could be leveraged for other applications, either multi-campus or single-campus. The licensing model for Duo covered us for usage by all employees and students, providing good financial efficiencies for the campuses. The technology is flexible enough to be implemented in a wide variety of platforms and use-cases. There were not any other immediate use-cases to integrate into the requirements process, so this aspect was a broad assessment of apparent flexibility of the tool.

Part of the process of acquiring Duo was getting an InCommon membership that covered all of our campuses. This required a bit of back-and-forth as each campus runs an independent IdP, which differed from some of the other InCommon multi-campus members.

## Implementation

The implementation team consisted of members in the following roles:

* Middleware manager – PM, GH vendor management, managed functional and data integration processes
* Information security director – Duo config and vendor management, stakeholder management, procurement process
* Portal developer – functional integration of GH and Duo
* Integrations developer – data feed from HR to Duo via OSB and MDM
* Middleware director – stakeholder management
* Enterprise architect/integrations manager – integrations design
* IAM manager – long-term service owner
* HR communications lead – comm plan, author, execution of comm plan
* HR stakeholders – guidance and decisions

Implementation fell into four main areas: deployment and configuration of GreyHeller ERP firewall, configuration of Duo MFA, data integration between CU systems and Duo, and functional integration of ERP Firewall and Duo.

Of these, integration between ERP Firewall and Duo proved the most labor intensive as GreyHeller had less experience in this area than expected, meaning more effort from the CU team to make that integration work. The concept was fairly simple, require Duo MFA when users access one of the designated PeopleSoft pages in HR self-service. This required ERP Firewall to make a call out to the Duo API to provide the username and trigger an MFA authentication attempt that was displayed within the PeopleSoft application window.

The data integration process relies on existing Oracle Service Bus and Master Data Management services to make real-time updates for new employees and changes to existing employee data. This work required addressing a data issues like which set of people to bring over, initial data population, updating data, formatting of international phone numbers, data to place in notes field, etc. When an employee record is added or updated in HRMS, this triggers a message on the service bus that is fed into a API call to Duo to add/update data.

We initially planned to do our bulk load via CSV file import, but discovered Duo had limitations on the size of the import files and didn’t handle data errors well. In the end, we used the API and a process similar to our data updates to do the initial data load.

Base configuration of Duo was fairly simple, although we had the added complexity of requesting separate sub-accounts for each of our campuses so they could manage their own implementations of Duo for other applications.

Here is a screenshot of the step-up authentication as it appears to a user who has just clicked to access their W2.



We are leveraging a customer-written Python script and the Duo API to pull Duo logs into our QRadar SIEM.

The HR self-service mutifactor system went live on July 18, 2014.

## Communications

The Employee Services department in the University of Colorado provided significant communications to stakeholders and end-users. Communication about updating phone numbers began two months before launch, including four emails to all employees, the pop-up at portal login, articles in multiple newsletters and communications to IT service desks. Communication to end-users about using multifactor began about a month before launch including the website, email, portal banners, video and posters. You can see the Employee Services website about multifactor, including the video, here: <http://www.cu.edu/employee-services/it-takes-two-portal-security-strengthened-new-tool>


## Lessons learned and next steps

Overall, the project was very successful, largely due to strong stakeholder engagement, executive support, existing project management structure, and good communication both within the team and with customers. Very few support calls were received and most were related to people who did not update their contact phone numbers prior to launch.

We did encounter some Duo admin user interface issues when dealing with large quantities of users, devices and log data. Duo implemented better data handling in the UI to address these issues. We (along with many other customers) also provided feedback about the lack of user self-service and the lack of delegated admin roles. Both of these features have been released by Duo since our launch.

As is true with many data integrations, we encountered a few hiccups in the data updates that required a few fixes, but the integrations team addressed these issues.

**Usage level:** Given the data behind multifactor (W2, W4, Direct Deposit, phone number changes), we expected a fairly steady low level of authentications all year, with a peak for tax season. That is exactly what we saw with daily usage around 100-200 successful authentications per day prior to tax season and a peak of more than 2000 successful authentications in one day when W2 posting was announced.

In the nine months since the launch, 21,000+ people have used MFA with a total of 52,000+ successful authentications. With the mix of SMS and voice, and the failure rate noted below, that amounts to about 100,000 credits used in nine months: only $1000 in telephony expenses.

**Failure rate:** We see a fairly consistent 16.5% MFA failure rate over months of use. We believe this failure rate stays consistent because the very infrequent use means there isn’t a learning curve. The errors appear to largely be one of two causes: the first is simply clicking submit without taking any action (~40% of failures) and the second is choosing to receive a verification call without paying attention to the phone number that is selected by default.

**Voice vs SMS:** We had guessed that users would favor using SMS messages over voice calls, but found that 55% of the successful authentications used the voice call method (45% SMS).

**Expanding use:** Use of multifactor is spreading in two ways at CU: expanding use within PeopleSoft and use in other applications. Within PeopleSoft we are looking to expand multifactor to student self-service and for privileged users. Both of these efforts are still in the early stages as we work with stakeholders and plan around a major PeopleSoft upgrade occurring this year. Use in other applications has begun on a couple of CU campuses, leveraging Duo for MFA on LastPass Enterprise for IT staff on one campus, and protecting remote desktop connections on some critical servers on another campus. A campus is also looking at replacing an existing Vasco token system for Linux shell access. Multiple campuses are considering how to best leverage Duo for their VPN services as well.

**Service refinement**: As Duo and GreyHeller continue to develop their products, more features are coming available that we are investigating. On the Duo side, we now have the ability to delegate subsets of admin features for groups like the HR and IT services desks. We are also considering taking a different approach with device management if we add MFA to self-service for students because Duo has added user device self-service. On the GreyHeller side, we are investigating their new features for field-level redaction with step-up authentication for displaying sensitive information. This would allow a user to see a screen of information and only be prompted for MFA if they wished to view a particular field (like SSN).