რა არის ციფრული ხელმოწერა?

შესავალი

საქართველოში ინტენსიურად ინერგება თანამედროვე ციფრული ტექნოლოგიები და მათთან დაკავშირებული სისტემები. ამის ერთ-ერთი მაგალითია ID ბარათი და მასთან დაკავშირებული სხვადასხვა სერვისი (**http://www.id.ge**). ამ შემთხვევაში ჩვენთვის საინტერესოა ID ბარათთან დაკავშირებული ციფრული ხელმოწერის სერვისი (იხ. **http://www.id.ge/signature.htm**, ასევე - ციფრული ხელმოწერის პორტალი **https://id.ge/signem-portal/**). კერძოდ, ის მათემატიკური აპარატი, რომელსაც ციფრული ხელმოწერის სისტემა ეფუძნება.

ციფრული ხელმოწერა ჩვეულებრივი ხელმოწერის ელექტრონული ეკვივალენტია. მისი დანიშნულებაა ელექტრონული დოკუმენტის ავთენტურობის (მისი და ორიგინალის იდენტურობის, მასში არასანქცირებული ცვლილებების არარსებობის, გაყალბების არარსებობის) დადასტურება. შეიძლება ითქვას, რომ ციფრული ხელმოწერა მასალის უსაფრთხოებას გაცილებით მეტად უზრუნველყოფს, ვიდრე ჩვეულებრივი.

ბანკები და მსგავსი დაწესებულებები ხშირად იყენებენ კლიენტების ჩვეულებრივი ხელმოწერის ნიმუშების შენახვის მეთოდს. ზოგჯერ ისინი უფრო შორსაც მიდიან: მაგალითად, არსებობს ბიომეტრიული ანალიზის მეთოდები, რომელთა საშუალებითაც ხდება კლიენტის ხელწერის სიჩქარის ან კალმის დაწოლის სიძლიერის ჩაწერა და შენახვა, ამ მონაცემებს კი მომავალში კლიენტის საიდენტიფიკაციოდ იყენებენ. მართალია, ამ შემთხვევაშიც მონაცემების აღნუსხვისა და შენახვის ციფრული მეთოდები გამოიყენება, მაგრამ ეს მაინც არ არის ის, რასაც ციფრულ ხელმოწერას ვუწოდებთ.

დასაწყისშივე შევნიშნავთ, რომ, გარდა უსაფრთხოების გაცილებით მაღალი დონისა, ციფრული ხელმოწერა ტრადიციული ხელმოწერის დამუშავებისა და შენახვის საშუალებებზე გაცილებით იაფიცაა. ეს კიდევ ერთი მაგალითია იმისა, როგორ აიაფებს ტექნოლოგიებისა და ინტელექტუალური მიღწევების გამოყენება სხვადასხვა სერვისს.

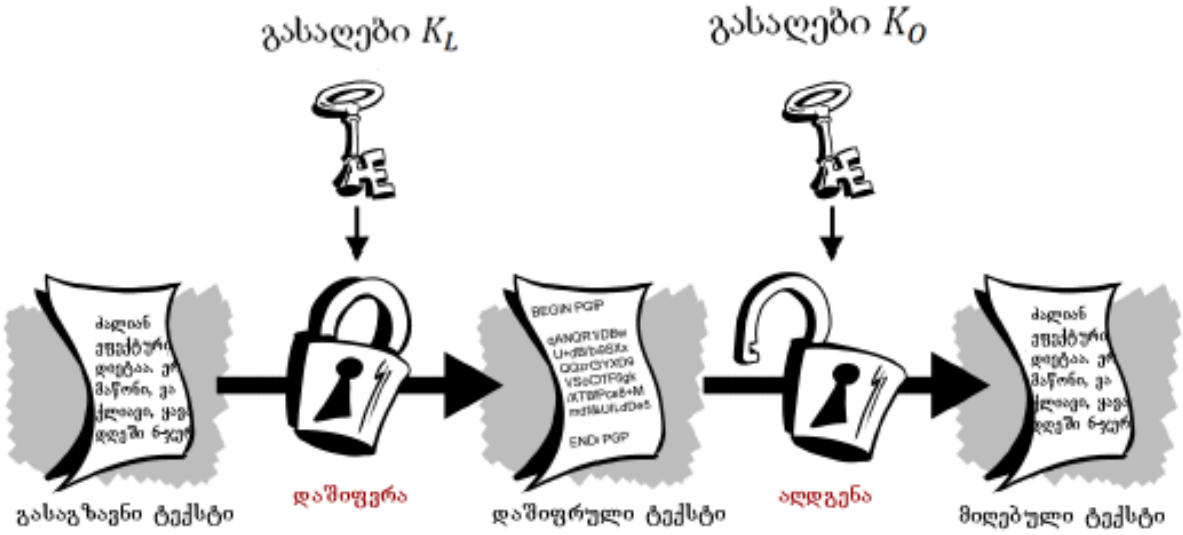
ციფრული ხელმოწერის სქემა, როგორც წესი, იყენებს ღია გასაღებით დაშიფვრის (**Public Key Encryption**) მეთოდს, რომელიც ასევე გამოიყენება მონაცემთა გადაცემისა და შენახვის დროს.

მონაცემთა დაშიფვრა ღია გასაღებით

მონაცემთა დაშიფვრას უმთავრესად მათი გადაცემის დროს იყენებენ არასანქცირებული წვდომისგან დასაცავად. ღია გასაღებით დაშიფვრისას გამოიყენება ორი „გასაღები“ (შეიძლება ითქვას, რომ ეს არის ორი „ძალიან დიდი“ რიცხვი). ერთ-ერთი მათგანია ე.წ. საიდუმლო გასაღები (Private Key), რომელიც ცნობილია მხოლოდ მისთვის, ვინც დაშიფრული მონაცემები უნდა წაიკითხოს. მეორეა ე.წ. ღია გასაღები (Public/Open Key), რომელიც არ არის დაფარული და ნებისმიერისთვის შეიძლება გახდეს ცნობილი.

ამ ორი გასაღების გამოყენებით მონაცემების დაშიფვრისა და წაკითხვის ზოგადი სქემის მეტაფორული წარმოდგენა ასეთია: ვთქვათ, ნანას სურს, დათოს გადაუგზავნოს დაშიფრული ტექსტი ისე, რომ ვერავინ შეძლოს მისი წაკითხვა, თუნდაც ამ მონაცემების ხელში ჩაგდება მოხერხოს.

წარმოვიდგინოთ, რომ დათოს აქვს ყუთი, რომელსაც აქვს საკეტი და ორი გასაღები - K_L და K_O. ამასთან, K_L გასაღები ყუთს მხოლოდ კეტავს, მისი გაღება კი არ შეუძლია; ყუთს აღებს მხოლოდ K_O გასაღები. დათოს აქვს ორივე გასაღები. თუ მას სურს, მიიღოს ვინმესგან - ამ შემთხვევაში, ნანასგან - საიდუმლო შეტყობინება, უგზავნის მას ყუთს და K_L გასაღებს (რა თქმა უნდა, ყუთი არ არის ჩაკეტილი); ნანა შეტყობინებას ათავსებს ყუთში, კეტავს მას K_L გასაღებით და უკანვე უგზავნის დათოს.



ამ გაგზავნა-გამოგზავნის პროცესში ვინმემ შესაძლოა ხელში ჩაიგდოს K_L გასაღები ან დაამზადოს მისი მისი ასლი, მაგრამ ის უკვე უსარგებლო იქნება, რადგან, როგორც თავიდანვე აღვნიშნეთ, ამ გასაღებით შესაძლებელია ყუთის მხოლოდ ჩაკეტვა. როდესაც დათო მიიღებს გზავნილს, გააღებს საკეტს K_O გასაღებით, ამოიღებს და წაიკითხავს წერილს.

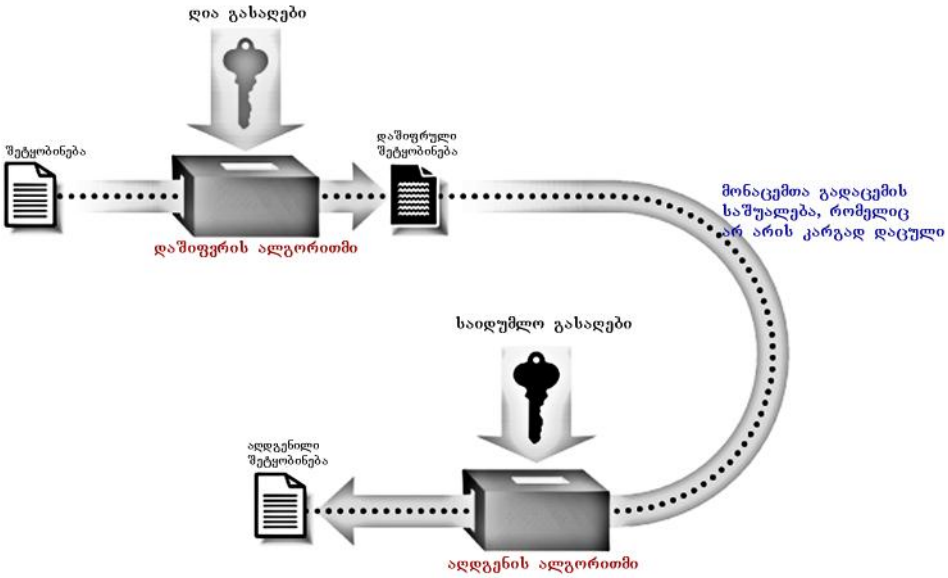
ამ სქემის მათემატიკური წარმოდგენა ეფუძნება ასახვის ცნებას. როგორც ცნობილია, ციფრულ სამყაროში ყოველგვარი მონაცემი: ტექსტი, გამოსახულება, ვიდეო- თუ აუდიომასალა, - რიცხვების საშუალებით გამოისახება, ამიტომ როდესაც ვამბობთ, რომ ერთ სუბიექტს სურს, მეორეს ამა თუ იმ სახის მონაცემი გაუგზავნოს, ვგულისხმობთ, რომ მას სურს ამ მონაცემის შესაბამისი რიცხვის გაგზავნა. გასაგზავნი რიცხვი შეიძლება იყოს ძალიან დიდიც - გააჩნია, რა სახისა და მოცულობისაა გასაგზავნი მასალა. მონაცემის დაშიფვრა კი იმას ნიშნავს, რომ გასაგზავნი რიცხვი რაიმე წესით სხვა რიცხვით შეიცვლება და ასე სახეცვლილი გაიგზავნება. მიმღებმა იცის დაშიფვრის წესის შებრუნებული წესი, რომლის გამოყენებითაც აღადგენს ორიგინალს.

მათემატიკურ ენაზე ეს ნიშნავს იმას, რომ გვაქვს რაღაც E ფუნქცია (დაშიფვრის ფუნქცია), რომელიც მოცემულ რიცხვს შეუსაბამებს სხვა რიცხვს. თუ ნანას სურს, დათოს გაუგზავნოს რაღაც x რიცხვი (შეტყობინება), იგი ამ რიცხვის ნაცვლად უგზავნის $y = E(x)$-ს. დათომ იცის

როგორია E ფუნქციის შექცეული ფუნქცია E^{-1}. იგი მიღებულ რიცხვზე ამოქმედებს მას და აღადგენს შეტყობინებას: $E^{-1}(y) = E^{-1}\big(E(x)\big) = x$. მაგალითად, წარმოვიდგინოთ რომ ნანას სურს დათოს გაუგზავნოს რიცხვი 147. დაშიფვრის ფუნქცია იყოს $E(x) = x^2$. მისი გამოყენებით ნანა გაუგზავნის არა 147-ს, არამედ $E(147) = 147^2 = 21609$-ს. დათომ იცის რომ მიღებულ რიცხვზე უნდა ამოქმედოს $E(x) = x^2$ -ის შექცეული ფუნქცია, რომელიც არის $E^{-1}(y) = \sqrt{y}$. ესე იგი, მიღებული რიცხვიდან უნდა ამოიღოს ფესვი.

ერთი შეხედვით, ეს ყოველივე ძალზე ადვილი ჩანს, მაგრამ ამ სქემის ნაკლი ის არის, რომ დაშიფვრის ფუნქცია მარტივი სახისაა. კერძოდ, ძალიან ადვილია მისი შექცეული ფუნქციის პოვნა და მისი საშუალებით საწყისი მონაცემის დადგენა. ამგვარად, თუ შემთხვევით ვინმეს ხელში ჩაუვარდა დაშიფრული მონაცემი და დაშიფვრის წესი (ამ შემთხვევაში - კვადრატში აყვანა), კვადრატული ფესვის ამოღებით იგი ადვილად მოახერხებს საწყისი მონაცემის დადგენას.

მონაცემთა დაშიფვრის პრაქტიკაში გავრცელებული ხერხის არსი იმაში მდგომარეობს, რომ მასში გამოყენებული დაშიფვრის ფუნქციისთვის ძალიან ძნელია შექცეული ფუნქციის აგება. ასე რომ, შესაძლოა ვინმეს ჰქონდეს დაშიფრული მონაცემი და იცოდეს დაშიფვრის ფუნქცია, მაგრამ საწყისი მონაცემის აღსადგენად მან უნდა იპოვოს დაშიფვრის ფუნქციის შექცეული ფუნქცია, რაც ძალიან რთული ამოცანაა. ამ შემთხვევაში შეფასება „ძალიან რთული“ ნიშნავს იმას, რომ შეუძლებელია ამ ამოცანის დროის მცირე შუალედში გადაჭრა დღეს არსებული მრავალი მაღალი წარმადობის კომპიუტერის ერთობლივი მუშაობითაც კი.



ეს სქემა ეფუძნება ძალზე საინტერესო (და არცთუ ისე რთულ) მათემატიკურ პროცედურას, რომელიც, თავის მხრივ, იყენებს ნაშთების თეორიის ელემენტებს, რაც სასკოლო მათემატიკის ერთ-ერთი შემადგენელი ნაწილია. სქემა იყენებს ალგორითმს, რომელსაც ეწოდება **ღია გასაღებით დაშიფვრის ალგორითმი**. ამ ალგორითმის აღწერა ხელმისაწვდომი გახდა 1978 წელს. მას ხშირად უწოდებენ RSA ალგორითმს - აბრევიატურა მიღებულია

მასაჩუსეტსის ტექნოლოგიების ინსტიტუტის იმ სამი მეცნიერის გვარების პირველი ასოებისგან, რომლებმაც ეს ალგორითმი აღწერეს (Ron Rivest, Adi Shamir, Leonard Adleman). RSA დაშიფვრის სქემა მონაცემთა დაშიფვრის ყველაზე გავრცელებული ხერხია. მას იყენებენ თითქმის ყველა ისეთ სისტემაში (საბანკო, სამხედრო, სამთავრობო და უბრალოდ სამომხმარებლო), რომლებშიც ზოგიერთი სახის მონაცემთა დაცულობა მნიშვნელოვანია.

ამ სქემასთან დაკავშირებული მათემატიკური აპარატის დეტალური აღწერა შეგიძლიათ იხილოთ ამ მისამართებზე:

. http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-045j-automata-computability-and-complexity-spring-2011/lecture-notes/MIT6_045JS11_rsa.pdf

. http://ocw.mit.edu/courses/mathematics/18-304-undergraduate-seminar-in-discrete-mathematics-spring-2006/projects/rsa_robles.pdf

ციფრული ხელმოწერა

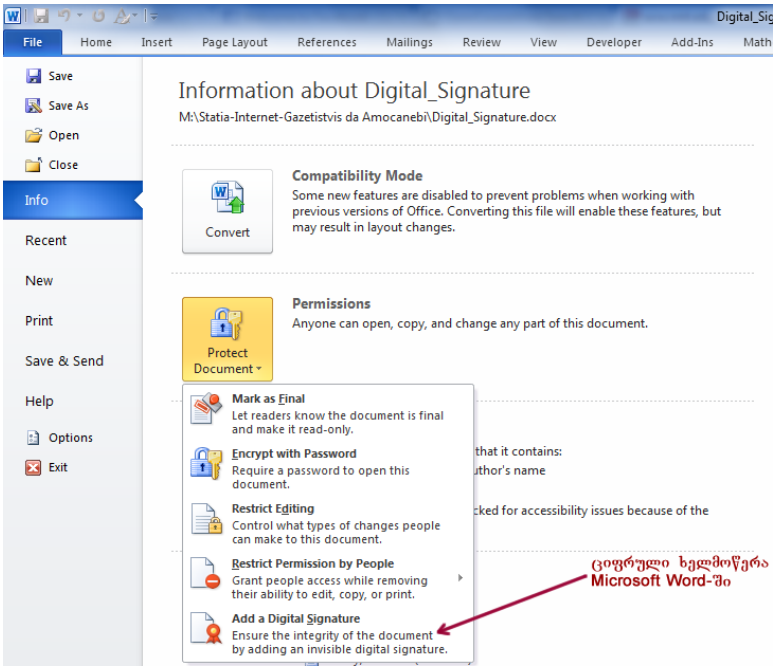
შეიძლება ითქვას, რომ ციფრული ხელმოწერა მონაცემთა დაშიფვრის შებრუნებული ოპერაციაა. თუ დაშიფვრის ძირითადი ამოცანაა მონაცემთა ორიგინალური ვერსიის დამალვა, ხელმოწერის მიზანია არა დამალვა, არამედ მონაცემთა ორიგინალურობის დადასტურება. კერძოდ, როდესაც თქვენ ჩვეულებრივი კალმით ხელს აწერთ რომელიმე დოკუმენტს, ამით მის ორიგინალურობას ადასტურებთ. ის შეიძლება იყოს ან არ იყოს თქვენი შექმნილი; მთავარი ის არის, რომ ხელმოწერით ადასტურებთ ამ მასალის შესაბამისობას იმ მასალასთან, რომელიც ხელმოწერის მომენტში თქვენ წინ იდო. მაგალითად, როდესაც მხატვარი ხელს აწერს თავის ნახატს, მას სურს, რომ ნახატს ყოველთვის თან ახლდეს მისი ორიგინალურობის დამადასტურებელი ნიშანი. როდესაც ხელშეკრულების გაფორმებისას მხარეები ხელს აწერენ ხელშეკრულების ტექსტს, ამით ისინი ადასტურებენ არა მხოლოდ იმას, რომ ეთანხმებიან ხელშეკრულების პირობებს, არამედ ეს არის მცდელობა იმისა, რომ ხელშეკრულების ტექსტი დაცული იყოს შემდგომი არასანქცირებული ცვლილებებისგან.

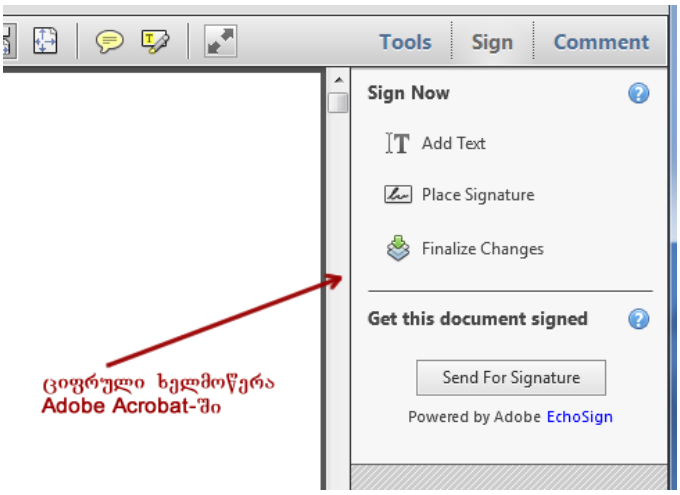
ალბათ ყველა ჩვენგანს ჰქონია ამ სახის ხელმოწერის გამოყენების შემთხვევა და ვიცით, რამდენად დაუცველია ხელმოწერის ასეთი არქაული ფორმა. უფრო მეტიც - ზოგჯერ იყენებენ ხელმოწერის ისეთ კიდევ უფრო დაუცველ ფორმას, როგორიცაა ელექტრონულ დოკუმენტში ჩასმული კალმით შესრულებული ხელმოწერის გრაფიკული ასლი (ამ სახის „ხელმოწერა“ ზოგიერთს ციფრულ ხელმოწერადაც კი მიაჩნია).

როგორც აღვნიშნეთ, ციფრულ ხელმოწერას საფუძვლად უდევს ღია გასაღებით დაშიფვრის ალგორითმი. ამ შემთხვევაში მისი სქემა ასეთია: დავუშვათ, თქვენ შექმენით რაიმე სახის ციფრული მასალა (ტექსტი, გრაფიკული, ვიდეო-, აუდიო მასალა) და გსურთ, ამ მასალას დაურთოთ თქვენი ხელმოწერა, რომელიც საჭიროების შემთხვევაში დაადასტურებს მის ორიგინალობას (იმას, რომ ამ მასალის ავტორი მართლაც თქვენ ხართ). როგორც უკვე ითქვა, ციფრული მასალა შეიძლება წარმოვადგინოთ რიცხვის სახით. ასე რომ, თქვენ მიერ შექმნილ ციფრულ მასალას შეესაბამება რაღაც რიცხვი x (მას უწოდებენ ამ მასალის დაიჯესტს, digest). თქვენ ამზადებთ ამ რიცხვის დაშიფრულ ვერსიას საკუთარი საიდუმლო გასაღების (მათემატიკურ ენაზე რომ ვთქვათ - ფუნქციის) საშუალებით: $y = E(x)$. ამის შემდეგ ციფრულ მასალას თან ურთავთ ამ დაშიფრულ დაიჯესტს, რომელიც არის ციფრული ხელმოწერა: $(x,\ E(x))$. ეს ხელმოწერა ციფრულ დოკუმენტში უხილავადაა ინტეგრირებული,

მაშინ როდესაც თქვენ მიერ შექმნილი მასალა ყველასათვის ხილულია. თუ მოხდა ისე, რომ გაყალბების მიზნით ვინმემ შეიტანა ცვლილებები მასალის ორიგინალში, თქვენ ყოველთვის შეგიძლიათ ამის დასაბუთება. თუ მოახდენთ გაყალბებული ნიმუშის, x'-ის (უფრო ზუსტად - მისი დაიჯესტის) დაშიფვრას მხოლოდ თქვენთვის ცნობილი დაფარული გასაღების (დაშიფვრის ფუნქციის) საშუალებით - $y' = E(x')$, აღმოჩნდება, რომ იგი არ ემთხვევა ორიგინალის დაშიფრულ ვერსიას: $y \neq y'$. უფრო მეტიც, მასალას, მის ციფრულ ხელმოწერასთან ერთად, შეიძლება დაურთოთ დაშიფვრის ფუნქციის შექცეული ფუნქცია E^{-1}. მისი გამოყენებით, მასალის ორიგინალობაში დარწმუნების მიზნით, ნებისმიერს შეეძლება ხელმოწერის დაიჯესტის აღდგენა და მისი შედარება მასალის დაიჯესტთან. თუ ვინმეს სურს მასალის სრულყოფილი გაყალბება, მაშინ მან უნდა იცოდეს დაშიფვრის ფუნქცია E. ამ შემთხვევაში გამყალბებელი ასე მოიქცევა: იგი შეიტანს ცვლილებებს მასალის ორიგინალში (x-ის მაგივრად, x'); დაშიფრავს ამ შეცვლილ ვერსიას, მისთვის ცნობილი დაშიფვრის ფუნქციით ($E(x')$) და ბოლოს, შეცვლილ მონაცემებს თან დაურთავს ამ გაყალბებულ ხელმოწერას: $(x',\ y' = E(x'))$. ამ შემთხვევაში თქვენ ვერ დაასაბუთებთ, რომ მასალა გაყალბებულია, რადგან მისი თანდართული ციფრული ხელმოწერა იმავე დაშიფვრის ფუნქციითაა მიღებული, რომელსაც თქვენ იყენებთ ხელმოწერის დროს. მაგრამ ციფრული ხელმოწერის არსი იმაში მდგომარეობს, რომ, ისევე როგორც მონაცემთა დაშიფვრის დროს, ძალიან ძნელია იმ ფუნქციის ამოცნობა, რომელსაც თქვენ იყენებთ ხელმოწერის მიზნით. ძნელია მაშინაც კი, როდესაც გამყალბებლისთვის ცნობილია მისი შექცეული ფუნქცია.

რა თქმა უნდა, სინამდვილეში ყოველივე ზემოაღწერილის რეალიზაცია ხდება სპეციალური კომპიუტერული პროგრამების საშუალებით. ასე რომ, მომხმარებელს არავითარი შეხება არ აქვს იმ დიდ რიცხვებსა და რთულ გამოთვლებთან, რომლებიც სრულდება დაშიფვრისა და ციფრული ხელმოწერის პროცედურების დროს. ასეთი დამატებითი ფუნქციები თან ერთვის თითქმის ყველა საოფისე და ინტერნეტ პროგრამულ უზრუნველყოფას (იხ. ნახ.)




Tools
Sign
Comment
Sign Now
Add Text
Place Signature
Finalize Changes
Get this document signed
Send For Signature
Powered by Adobe EchoSign
ციფრული ხელმოწერა
Adobe Acrobat-ში