Pengembangan Skema Verifikasi dan Validasi pada E-Voting dan E-Recap untuk Indonesia yang Berbasis Message Authentication Codes (MAC) dan Public Key Infrastructure (PKI) = Development of E-Voting and E-Recap Verification and Validation Schemes for Indonesia Based on Message Authentication Codes (MAC) and Public Key Infrastructure (PKI).

Sihite, Alfonso Brolin, author

Abstrak

ABSTRAK
Pemilu konvensional memiliki banyak kekurangan, beberapa di antaranya adalah perhitungan real count yang lama, biaya pencetakan kertas surat suara dan biaya distribusinya baik dari pusat ke daerah maupun sebaliknya yang besar, kemungkinan terjadinya kekurangan kertas suara saat pemilu berlangsung, kemungkinan terjadinya kecurangan terjadi karena satu orang memberikan suara lebih dari satu kali, dan lain-lain. Melihat hal tersebut, penggunaan teknologi e-voting dalam proses pemilihan umum (pemilu) diyakini dapat membuat penyelenggaraan pemilu menjadi efektif dan efisien. Pada penelitian ini dilakukan pengembangan skema verifikasi dan validasi e-voting yang dapat mengatasi masalah-masalah yang mungkin terjadi dalam pemilu konvensional tersebut dan tetap memenuhi asas-asas yang terdapat dalam pemilu di Indonesia, yaitu Luber Jurdil (Langsung, Umum, Bebas, Rahasia, Jujur, dan Adil). Sistem e-voting dilengkapi dengan e-recap yang juga berfungsi untuk verifikasi suara sehingga seluruh masyarakat dapat melihat, memeriksa, dan mengontrol hasil dari sistem e-voting ini. Skema e-voting dan e-recap ini berbasis penerapan Message Authentication Codes (MAC) dan Public Key Infrastructure (PKI) dengan tujuan pada hasil rekapitulasi, tidak tercantum siapa pemilih dan suara yang diberikan sehingga tetap memenuhi asas rahasia dalam pemilu, namun seluruh suara dapat terkumpul dan terverifikasi kebenarannya. Pemilih sendiri bisa melakukan verifikasi terhadap suara yang telah diberikan agar tidak ada modifikasi suara saat masuk ke sistem e-recap sehingga pemilu tetap dapat berlangsung transparan, akuntabel, dan dapat diuji oleh publik. Penelitian ini melakukan pembuktian skema dengan menerapkan algoritma HMAC yang dikonstruksi dengan fungsi hash SHA3. Hal ini dilakukan sebagai pembuktian apakah terdapat collision pada skema e-voting dan e-recap yang menggunakan algoritma HMAC SHA3-256. Hasil pembuktian menyatakan bahwa dengan 10 juta sampel yang digunakan, tidak ditemukan collision pada skema e-voting dan e-recap yang menggunakan algoritma HMAC SHA3-256. Hal tersebut menunjukkan bahwa skema verifikasi dan validasi pada e-voting dan e-recap ini tidak akan menimbulkan collision sehingga masing-masing pemilih akan mendapatkan vote code yang unik. Dengan begitu, diharapkan dengan skema verifikasi dan validasi pada e-voting dan e-recap ini, pemilu secara konvensional dapat diganti dengan sistem e-voting, namun tetap memenuhi asas-asas yang terdapat dalam pemilu, yaitu Luber Jurdil (Langsung, Umum, Bebas, Rahasia, Jujur, dan Adil). Selain itu, pemilu tetap dapat berlangsung transparan, akuntabel, dan dapat diuji oleh publik.
<hr>
ABSTRACT
Conventional elections have many shortcomings, some of them are the calculation of a real count that takes

a long time, the big costs of printing ballot papers and distribution costs both from the center to the regions and vice versa, the possibility of ballot paper shortages during the election, the possibility of fraud occurs because one person votes more than once, et cetera. Seeing this, the use of e-voting technology in the general election process is believed to be able to make the election effective and efficient. This research aims to develop an e-voting verification and validation scheme that can solve these problems that might occur in conventional elections and still fulfill the election principles of Indonesia, namely Direct, General, Free, Confidential, Honest, and Fair. The e-voting system is equipped with an e-recap system which has a function for ballot verification so that all of the people can see, examine, and control the results of this e-voting system. This e-voting and e-recap scheme is based on the application of Message Authentication Codes (MAC) and Public Key Infrastructure (PKI) with the aim is in the recapitulation results, there is not listed who the voters are and the votes given so that they still fulfill the confidential principles in elections, but all votes can be collected and verified. The voters themselves can verify the vote that has been given, so that there is no vote modification when entering the e-recap system. Thus, the election can be transparent, accountable, and can be examined by the public. This research proves the scheme by applying the HMAC algorithm which is constructed with the SHA3 hash function. This is done as a proof whether there is a collision in the e-voting and e-recap scheme using the HMAC SHA3-256 algorithm. The results show that with 10 million samples used, no collision was found in the e-voting and e-recap scheme using the HMAC SHA3-256 algorithm. This shows that the verification and validation scheme in e-voting and e-recap will not cause collisions so that each voter will get a unique vote code. Thus, it is expected that with this verification and validation scheme on e-voting and e-recap, conventional elections can be replaced with an e-voting system, but still fulfill the election principles of Indonesia, such as Direct, General, Free, Confidential, Honest, and Fair. In addition, the election can still be transparent, accountable, and can be examined by the public.